



JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2000032056 A**

(43) Date of publication of application: **28.01.00**

(51) Int. Cl. **H04L 12/56**
H04L 12/46
H04L 12/28
H04L 12/66

(21) Application number: **10210387**

(22) Date of filing: 09.07.98

(71) Applicant: **NEC CORP**

(72) Inventor: **YAMADA KENSHIN
SERA TAKAFUMI
ARUTAKI AKIRA**

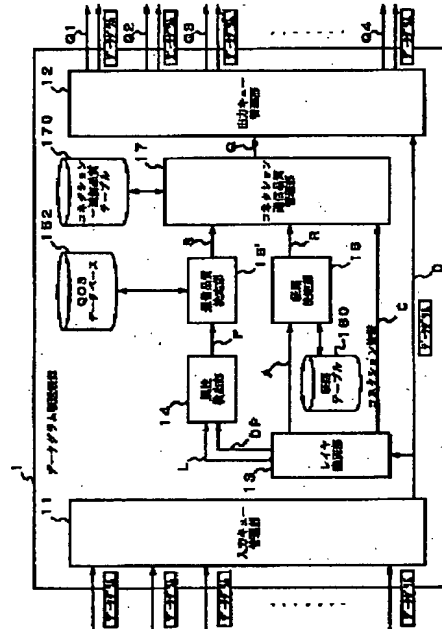
(54) COMMUNICATION QUALITY CONTROLLER

(57) Abstract:

PROBLEM TO BE SOLVED: To provide the communication quality controller that decides optimum communication quality from a received datagram and transfers it.

SOLUTION: An attribute detection section 14 extracts attribute information of communication from information of a protocol layer or any layer and a communication quality decision section 15 and a connection communication quality management section 17 decides the communication quality for the transmission of the datagram according to quality information of connection corresponding to the extracted attribute information in addition to decision of a destination by data below the protocol layer included in the datagram.

COPYRIGHT: (C)2000,JPO



FA-00EC0174

(2) 特開2000-032056

P-741

【特許請求の範囲】

【請求項1】 既存データネットワークのプロトコルレイヤを終端するネットワーク終端装置と、受信したデータグラムの通信の品質に基づいてプロトコルレイヤ3以下を終端するプロトコル終端装置と、プロトコルレイヤ3以下の通信の属性とこれら任意の終端装置で受信されたデータグラムに含まれるプロトコルレイヤ4、5、6、7の各々またはいずれかのレイヤの情報から導出される通信の属性に対応するコネクションの品質情報に従って指定された終端装置に対して前記データグラムを転送する通信データグラム転送装置とを有し、通信の属性に対応するコネクションの品質に最適なデータグラム転送機能を実現する通信品質制御装置において、

前記通信データグラム転送装置が、任意の終端装置で受信されたデータグラムのプロトコルレイヤ3以下のレイヤの情報に含まれる識別情報を検査すると同時にデータグラムのプロトコルレイヤ4、5、6、7の各々またはいずれかのレイヤの情報に含まれる識別情報と検査し各々のプロトコルレイヤの通信の属性情報を取り出す属性識別手段と、

前記データグラムがプロトコル終端装置で受信された場合に前記データグラムから導出された各々のプロトコルレイヤの通信の属性情報と、前記コネクションの品質情報からなる組に基づいてデータグラムを送信する通信品質を決定し、前記プロトコル終端装置に対して通知する通信品質決定手段とを備えることを特徴とする通信品質制御装置。

【請求項2】 既存データネットワークのプロトコルレイヤを終端するネットワーク終端装置と、受信したデータグラムの通信の品質に基づいてプロトコルレイヤ3以下を終端するプロトコル終端装置と、これら任意の終端装置で受信されたデータグラムに含まれるプロトコルレイヤ4、5、6、7の各々またはいずれかのレイヤの情報から導出される通信の属性とこれら任意の終端装置で受信されたデータグラムに含まれるプロトコルレイヤ4、5、6、7の各々またはいずれかのレイヤの情報に基づいて指定された終端装置に対して前記データグラムを転送する通信データグラム転送装置とを有し、通信の属性に対応するコネクションの品質に最適なデータグラム転送機能を実現する通信品質制御装置において、

前記通信データグラム転送装置が、任意の終端装置で受信されたデータグラムのプロトコルレイヤ4、5、6、7の各々またはいずれかのレイヤの情報に含まれる識別情報を検査し各々のプロトコルレイヤの通信の属性情報とこれら任意の終端装置で受信されたデータグラムから導出された各々のプロトコルレイヤの通信の属性情報と、前記コネクションの品質情報からなる組に基づいてデータグラムを送信する通信品質を決定し、前記プロトコル終端装置に対して通知する通信品質決定手段とを備えることを特徴とする通信品質制御装置。

制御装置。

【請求項3】 前記属性識別手段が、受信されたデータグラムより、前記レイヤ情報を識別すると共に、前記データグラムのコネクション識別情報よりコネクションの状態を識別してコネクション情報として前記通信品質決定手段に出力し、かつ前記データグラムの転送経路を決定し転送先経路情報として前記通信品質決定手段に出力し、

前記通信品質決定手段は、前記属性情報に対応するコネクションの品質情報と、前記転送先経路情報により、データグラムを送信する通信品質を決定することを特徴とする請求項1または請求項2に記載の通信品質制御装置。

【請求項4】 前記属性識別手段は、識別したコネクションの状態から、レイヤ4以上の属性を検出する必要があると判断した場合に、前記レイヤ情報と、前記データグラムの一部または全部に基づいて、通信の属性情報を取り出すことを特徴とする請求項3に記載の通信品質制御装置。

【請求項5】 前記通信データグラム転送装置が、コネクション情報と通信品質を組にして記録したコネクション通信品質データベースを備え、

前記通信品質決定手段は、前記コネクション情報と前記転送先経路情報、またはコネクション品質情報が入力した場合に、前記データグラムが前記コネクション通信品質データベースによる管理が必要かどうかを判断し、

管理が必要がある場合、前記コネクション通信品質データベースに同一のコネクションが存在するかを検査し、同一のコネクションが存在する場合、コネクション通信品質データベースを参照して通信品質を決定し、存在しない場合、前記コネクション情報と、前記コネクションの品質情報と、前記転送先経路情報により通信品質を決定しかつコネクション情報と通信品質を組にして前記コネクション通信品質データベースに記録し、

管理が必要ない場合、前記コネクション情報と前記転送先経路情報により通信品質を決定することを特徴とする請求項3または請求項4に記載の通信品質制御装置。

【請求項6】 前記属性情報に対応する前記コネクション品質情報を格納するデータベースを備え、

前記通信品質決定手段は、前記データベースを参照し、前記属性情報に基づいて前記コネクション品質情報を決定することを特徴とする請求項1乃至請求項5に記載の通信品質制御装置。

【請求項7】 レイヤ3をIPとし、レイヤ4をTCPとし、レイヤ5をHTTPとし、

(19) 日本国特許庁 (J P) (12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2000-32056
(P2000-32056A)
(43) 公開日 平成12年1月28日 (2000.1.28)

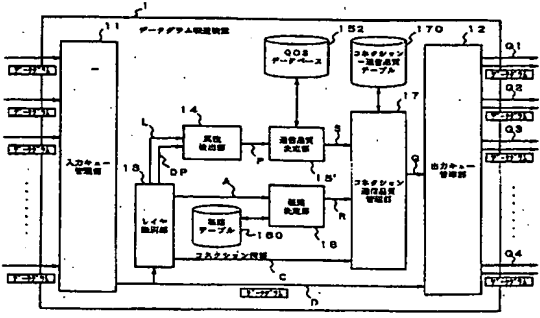
(51) Int. Cl. H04 L 12/56 12/48 12/28 12/66	識別記号 F1 H04 L 11/20 11/00 11/20	データ (参考) 102D 5K030 310C 5K033 B
---	---	---

(21) 出願番号 (22) 出願日 平成10年7月9日 (1998.7.9)	特願平10-210387 (71) 出願人 00004237 日本電気株式会社 東京都港区芝五丁目7番1号 (72) 発明者 山田 滋智 東京都港区芝五丁目7番1号 株式会社内 世良 孝文 東京都港区芝五丁目7番1号 株式会社内 (74) 代理人 100063695 弁理士 松本 正夫
---	---

(54) 【発明の名称】 通信品質制御装置

(57) 【要約】
【課題】 受信したデータグラムにおいて、最適な通信品質を決定しデータグラムを転送する通信品質制御装置を提供する。

【解決手段】 データグラムに含まれるプロトコルレイヤ3以下のデータにより送信先を決定するだけでなく、プロトコルレイヤ4、5、6、7の各々またはいずれかのレイヤの情報より通信の属性情報を属性検出部14により取り出し、取り出した属性情報と対応するコネクションの品質情報にしたがって通信品質決定部15及びコネクション通信品質管理部17にてデータグラムを送信する通信品質を決定する。



最狭に絞く

方法、HTTPヘッダに含まれるHostによりHTTPデータを要求されるホスト及びそのポート番号、HTTPヘッダに含まれるIf-RangeによりHTTPデータの取得条件、HTTPヘッダに含まれるPublicによりサーバの許可するMethod、HTTPヘッダに含まれるRangeによりサーバプログラムの要求しているHTTPデータのRangeの少なくとも1を検査することを特徴とする請求項7に記載の通信品質制御装置。

【請求項15】 前記属性識別手段が、前記識別情報として、受信データグラムのHTTPヘッダに含まれるContent-Lengthによりデータグラムのデータ長、HTTPヘッダに含まれるConnectionによりデータグラムのコネクションの状態、HTTPヘッダに含まれるWarningによりユーザプログラムに要求されるサーバの応答情報、HTTPヘッダに含まれるRefererにより要求されたHTTPデータを取得可能な日時、HTTPヘッダに含まれるViaによりバケットを中継してきたプロキシサーバまたはサーバエイトのフロントリバーシオン及びホスト名及び使用ソフトウェア名、HTTPヘッダに含まれるTransfer-Encodingによりデータグラムのコーデイング方法の少なくとも1を検査することを特徴とする請求項7に記載の通信品質制御装置。

【請求項16】 レイヤ3をIPとし、レイヤ4をTCPまたはUDP(User Datagram Protocol)として、前記属性識別手段は、前記データグラムのIPヘッダのフロントリバーシオン番号またはIPヘッダの次のヘッダ値を検査し、レイヤ4がTCPまたはUDPであることを認識するとともに、識別情報として受信データのTCPヘッダまたはUDPヘッダに含まれる一つまたは複数の識別情報を検査し、

前記通信品質決定手段は、前記データグラムがフロントリバーシオンに転送された場合に、前記データグラムより抽出されたコネクションに最適なレイヤ3以下のコネクションの品質を決定し、コネクションの品質に基づくデータグラム転送処理を行なうことにより、送信すべきデータグラムのコネクション品質を変えて制御することを特徴とする請求項1乃至請求項6に記載の通信品質制御装置。

【請求項17】 前記属性識別手段は、前記識別情報として、受信データグラムのUDPヘッダに含まれるchecksumフィールドを検査することとを特徴とする請求項16に記載の通信品質制御装置、

【請求項18】 レイヤ3をIPとし、レイヤ4をTCPまたはUDPとし、レイヤ5をDNSまたはFTPまたはSNMPとして、

前記属性識別手段は、前記データグラムのIPヘッダの

フロントリバーシオン番号、または該フロントリバーシオン番号と前記データグラムのTCPまたはUDPフロントリバーシオンポートアドレス、または前記データグラムのIPヘッダの次のヘッダ値、または該ヘッダ値と前記データグラムのTCPまたはUDPフロントリバーシオンポートアドレスを検査し、レイヤ5がDNSまたはFTPまたはSNMPであることを認識するとともに、識別情報として受信データのDNSメッセージ、TCPまたはUDPヘッダとDNSメッセージ、FTPメッセージ、UDPヘッダとFTPメッセージ、SNMPメッセージ、またはUDPヘッダとSNMPメッセージの何れかに含まれる一つまたは複数の識別情報を検査し、

前記通信品質決定手段は、前記データグラムがフロントリバーシオンに転送された場合に、前記データグラムより抽出されたコネクションに最適なレイヤ3以下のコネクションの品質を決定し、コネクションの品質に基づくデータグラム転送処理を行なうことにより、送信すべきデータグラムのコネクション品質を変えて制御することを特徴とする請求項1乃至請求項6に記載の通信品質制御装置。

【請求項19】 前記属性識別手段は、前記識別情報として、受信データグラムのDNSメッセージにquery typeが存在するかどうかを検査することを特徴とする請求項18に記載の通信品質制御装置。

【請求項20】 前記属性識別手段は、前記識別情報として、受信データグラムのFTPメッセージに含まれるopcodeを検査することを特徴とする請求項18に記載の通信品質制御装置。

【請求項21】 前記属性識別手段は、前記識別情報として、受信データグラムのSNMPメッセージに含まれるPDUタイプを検査することを特徴とする請求項18に記載の通信品質制御装置。

【請求項22】 レイヤ3をIPとし、レイヤ4をTCPとし、レイヤ5をFTPまたはSMTPまたはとして、

前記属性識別手段は、前記データグラムのIPヘッダのフロントリバーシオン番号と前記データグラムのTCPフロントリバーシオンポートアドレス、または前記データグラムのIPヘッダの次のヘッダ値、または該ヘッダ値と前記データグラムのTCPフロントリバーシオンポートアドレスを検査し、レイヤ5がFTPまたはSMTPであることを認識するとともに、識別情報として受信データのFTP Command、FTP Reply、TCPヘッダとFTP Command、またはFTP Reply、SMTP Command、SMTP Reply Code、SMTPヘッダ、TCPヘッダとSMTP CommandまたはSMTP Reply CodeまたはSMTPヘッダの何れかに含まれる一つまたは複数の識別情報を検査し、

コルヘッダ内のポートアドレス、または前記データグラムのIPヘッダの次のヘッダ値、または該ヘッダ値と前記データグラムのTCPフロントリバーシオンポートアドレスとを検査し、レイヤ5がHTTPであることを認識するとともに受信データグラムのTCPヘッダまたは、TCPヘッダ及びHTTPメッセージに含まれる一つまたは複数の識別情報を検査し、

前記通信品質決定手段は、前記データグラムがフロントリバーシオンに転送された場合に、前記データグラムより抽出されたコネクションに最適なレイヤ3以下のコネクションの品質を決定し、コネクションの品質に基づくデータグラム転送処理を行なうことにより、送信すべきデータグラムのコネクション品質を変えて制御することを特徴とする請求項1乃至請求項6に記載の通信品質制御装置。

【請求項8】 前記属性識別手段が、前記識別情報として、受信データグラムのHTTPヘッダに含まれるContent typeによりデータグラムのメディア属性、HTTPヘッダに含まれるFromフィールドによりデータグラムを送出したユーザの電子メールアドレス、HTTPヘッダに含まれるUser-Agentによりデータグラムを作成したユーザプログラム名及びVersion、HTTPヘッダに含まれるServerによりデータグラムを作成したサーバソフトウェア名及びVersionの少なくとも1を検査することを特徴とする請求項7に記載の通信品質制御装置。

【請求項9】 前記属性識別手段が、前記識別情報として、受信データグラムのHTTPヘッダに含まれるDateによりデータグラムの作成日時、HTTPヘッダに含まれるAuthorizationによりデータグラムの認証情報、当該認証情報の暗号化方法、HTTPヘッダに含まれるExpiresによりデータグラムの有効日時の少なくとも1を検査することを特徴とする請求項7に記載の通信品質制御装置。

【請求項10】 前記属性識別手段が、前記識別情報として、受信データグラムのHTTPヘッダに含まれるPragmaによりデータグラムの要求事項、HTTPヘッダに含まれるCache-Confioによりデータグラムのキャッシュ制御情報、HTTPヘッダに含まれるIf-Modified-SinceによりMethodの実行条件、HTTPヘッダに含まれるIf-Unmodified-SinceによりMethodの実行条件、HTTPヘッダに含まれるURI行(Request-Line)内のリソースURLによりクライアントの要求しているURL、HTTPヘッダに含まれるLast-ModifiedによりHTTPデータの最終更新日時の少なくとも1を検査することを特徴とする請求項7に記載の通信品質制御装置。

【請求項11】 前記属性識別手段が、前記識別情報として、受信データグラムのHTTPヘッダに含まれるRefererによりHTTPデータの参照元URI(Uniform Resource Identifier)、HTTPヘッダに含まれるLocationによりHTTPデータのデータのおかれているURL、HTTPヘッダに含まれるForwardedによりデータグラムの転送先URI及び転送元ドメインネーム、HTTPヘッダに含まれるContent-BasによりデータグラムのhasseURI、HTTPヘッダに含まれるContent-LocationによりHTTPデータの存在するURL、HTTPヘッダに含まれるMethodによりユーザプログラムからのHTTPデータ要求方法の少なくとも1を検査することを特徴とする請求項7に記載の通信品質制御装置。

【請求項12】 前記属性識別手段が、前記識別情報として、受信データグラムのHTTPヘッダに含まれるMIME-VersionによりデータグラムがMIME(Multipurpose Internet Mail Extensions)のVersion、HTTPヘッダに含まれるAcceptによりユーザプログラムの許可するメディア属性、HTTPヘッダに含まれるAccept-Charsetによりユーザプログラムの許可する文字セット、HTTPヘッダに含まれるAccept-Encodingによりユーザプログラムの許可するデータグラムのコーデイング方法、HTTPヘッダに含まれるAccept-Languageによりユーザプログラムの許可するデータグラムの言語、HTTPヘッダに含まれるContent-Encodingによりデータグラムのエンコード方法、HTTPヘッダに含まれるContent-Languageによりデータグラムの言語の少なくとも1を検査することを特徴とする請求項7に記載の通信品質制御装置。

【請求項13】 前記属性識別手段が、前記識別情報として、受信データグラムのHTTPヘッダに含まれるSiaus Codeによりユーザプログラムからの要求に対するサーバの応答内容、HTTPヘッダに含まれるWWW-Authenticateによりサーバの要求する認証情報、HTTPヘッダに含まれるProxy-Authenticatcによりプロキシサーバの要求する認証情報、HTTPヘッダに含まれるProxy-Authorizationによりデータグラムの認証情報の少なくとも1を検査することを特徴とする請求項7に記載の通信品質制御装置。

【請求項14】 前記属性識別手段が、前記識別情報として、受信データグラムのHTTPヘッダに含まれるAllowによりHTTPデータの許可するMethod、HTTPヘッダに含まれるAccept-Rangeによりサーバの許可するRange要求

よりデータグラムを転送しているからである。

【0009】より具体的に、以下のような問題点があった。

【0010】第1に、動画、音声、画像などの通信属性に基づいて、最適な通信品質でデータグラムの転送がでない。

【0011】第2に、特定のユーザや団体の使用するトランスファックに対してある通信品質を提供する場合、IPアドレス等の宛先アドレス、送信元アドレスを用いてのみならず、特定のユーザや団体を特定することができない。

【0012】第3に、通信属性により定まるコネクションの品質に応じた課金を行なうことができない。

【0013】第4に、データグラムがセキュリティ上非常に重要な情報を含んでいるかどうかを判別できないため、セキュリティ上重要な情報を含んだデータグラムと、そうでないデータグラムを同様の通信品質でデータグラム転送処理を行なってしまうため、セキュリティ品質に応じたデータグラム転送を実現することができない。

【0014】第5に、データグラムの新規性により、コネクション品質を決定することができない。

【0015】第6に、トランスポート層において規定されるコネクションにおいて、該コネクションの状態を判断し、該コネクションの通信品質を動的に変更することができない。

【0016】本発明の目的は、高速なレイヤ3以下のデータグラム転送機能を実現しながら、データグラムの通信の属性を認識し、抜き出された通信属性に最適な通信品質によりデータグラムを転送することを可能とする通信品質制御装置を提供することにある。

【0017】本発明の他の目的は、あらかじめ登録してあるユーザに対して高度かつ多様な通信サービスを実現でき、また、通信品質に応じた課金単位で課金を行なうことができる通信品質制御装置を提供することにある。

【0018】本発明の他の目的は、データグラムがセキュリティ上非常に重要なデータを含んでいるかどうかを判断し、データグラムに対応するセキュリティ品質に応じたデータ転送を実現できる通信品質制御装置を提供することにある。

【0019】本発明の他の目的は、データグラムの新規性を判断し、コネクションの品質を決定することができ、また、同一のコネクションで認識できる情報だけでなく、他のコネクションにおいて認識した情報を基にコネクション品質を決定し、最適な通信品質でデータグラムを転送可能である通信品質制御装置を提供することにある。

【0020】
【課題を解決するための手段】上記目的を達成する本発明は、既存データネットワークのプロトコルレイヤを終

端するネットワーク終端装置と、受信したデータグラムの通信の品質に基づいてプロトコルレイヤ3以下を転送するプロトコル終端装置と、プロトコルレイヤ3以下の通信の属性とこれら任意の終端装置で受信されたデータグラムに含まれるプロトコルレイヤ4、5、6、7の各々またはいずれかのレイヤの情報から導出される通信の属性に对应するコネクションの品質情報に従って指定された終端装置に対して前記データグラムを転送する通信品質制御装置とを有し、通信の属性に对应する通信品質制御装置において、前記通信データグラムの転送装置が、任意の終端装置で受信されたデータグラムのプロトコルレイヤ3以下のレイヤの情報に含まれる識別情報を検査すると同時にデータグラムのプロトコルレイヤ4、5、6、7の各々またはいずれかのレイヤの情報に含まれる識別情報を検査し、各々のプロトコルレイヤの通信の属性情報を取り出す属性識別手段と、前記データグラムがプロトコル終端装置で受信された場合に前記データグラムの属性情報と、前記コネクションの品質情報からなる組に基づいてデータグラムを送信する通信品質決定手段とを備えることを特徴とする。

【0021】また、請求項2の本発明は、既存データネットワークのプロトコルレイヤを終端するネットワーク終端装置と、受信したデータグラムの通信の品質に基づいてプロトコルレイヤ3以下を終端するプロトコル終端装置と、これら任意の終端装置で受信されたデータグラムに含まれるプロトコルレイヤ4、5、6、7の各々またはいずれかのレイヤの情報から導出される通信の属性に对应するコネクションの品質情報に従って指定された終端装置に対して前記データグラムを転送する通信品質制御装置において、前記通信データグラムの転送装置が、任意の終端装置で受信されたデータグラムのプロトコルレイヤ3以下のレイヤの情報に含まれる識別情報を検査すると同時にデータグラムのプロトコルレイヤ4、5、6、7の各々またはいずれかのレイヤの情報に含まれる識別情報を検査し、各々のプロトコルレイヤの通信の属性情報を取り出す属性識別手段と、前記データグラムがプロトコル終端装置で受信された場合に前記データグラムの属性情報と、前記コネクションの品質情報からなる組に基づいてデータグラムを送信する通信品質決定手段とを備えることを特徴とする。

【0022】このように、データグラムのプロトコルレイヤ4、5、6、7の各々またはいずれかのレイヤの情報に含まれる識別情報を検査し、各々のプロトコルレイヤの通信情報を取り出すことにより、より詳細に通信の属性を特定することができ、該通信の属性に最適なコネク

前記通信品質決定手段は、前記データグラムがプロトコル終端装置に転送された場合に、前記データグラムより導出されたコネクションに最適なレイヤ3以下のコネクションの品質を決定し、コネクションの品質に基づいてデータグラム転送処理を行なうことにより、送信すべきデータグラムのコネクション品質を変えて制御することを特徴とする請求項1乃至請求項6に記載の通信品質制御装置。

【請求項2】 転送の物理レイヤをATM転送方式とし、コネクション品質に基づきデータグラム転送処理としてATMの各々のコネクション品質に別々のVC (Virtual Circuit) を割り当ててデータグラムの転送を行ない、各々のVCはコネクション品質に応じた通信品質制御パラメータが設定されていることにより、データグラムから導出されるメディアの属性に応じた転送が行なわれることを特徴とする請求項1乃至請求項2に記載の通信品質制御装置。

【請求項24】 前記通信品質決定手段は、前記通信品質に加えて、コネクション設定のためのコネクション設定マッパシージに応じたコネクション設定ロバーストネスを選択して設定することを特徴とする請求項1乃至請求項23に記載の通信品質制御装置。

【請求項25】 前記通信品質決定手段は、前記属性情報により、前記コネクションの通信品質として、最適な帯域幅に関する制御パラメータ、最大遅延時間や遅延時間変動量を含む遅延時間に関する最適な制御パラメータ、バッファ量を含むデータ喪失に関する最適な制御パラメータ、最適な課金情報に関する制御パラメータ、最適なセキュリティ品質に関する制御パラメータのうち少なくとも1の制御パラメータを決定することとを特徴とする請求項1乃至請求項24に記載の通信品質制御装置。

【請求項26】 前記通信品質決定手段は、前記コネクションの通信品質に基づき、最適なデータグラムの転送先、最適なデータグラムの転送経路の少なくとも一方を決定することを特徴とする請求項1乃至請求項25に記載の通信品質制御装置。

【請求項27】 前記通信品質決定手段は、前記コネクションの通信品質に基づいて、必要に応じて専用の物理回線を該コネクションによって使用し、前記データグラムを暗号化または復号化して転送し、データグラム内の不要な情報を削除し、圧縮によりデータグラムのサイズを削減し、データグラムのトンネリングを行なうことを特徴とする請求項1乃至請求項26に記載の通信品質制御装置。

【請求項28】 前記通信品質決定手段は、前記属性情報によりコネクションの通信品質としてコネクション設定優先度またはコネクション転送優先度を設定し、該コネクション設定優先度の高いコネクションのコネクション設定処理を優先し、またはコネクション転送優先度の高いコネクションのデータグラムの転送を優先させることを特徴とする請求項請求項1乃至請求項27に記載の通信品質制御装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、ネットワークの通信装置に関し、特にデータグラムの転送網上で既存データネットワークに位置する通信品質制御装置に関する。

【0002】

【従来の技術】 従来の通信網においては、例えばLAN (Local Area Network) では、Ethernet 技術、ATM 技術などの物理転送技術に基づいて上位プロトコルであるIP、さらにTCPによってデータグラムの転送を行なっている。

【0003】 また、LANのIPサブネットワークを接続したインターネット (The Internet) においても、前述のEthernet 技術やATM 技術を組みとる各種物理転送方法が組み込まれ装置に実装されている。

【0004】 もともとこれらのネットワークでは、エンドーエンポイントにおける通信すなわちコネクションを保証するためのしくみであって、通信網内に位置するデータグラム中継転送する装置は、エンドーエンポイントの転送品質を満足するためには、あらかじめエンドーエンポイントのプロトコルの物理転送レイヤに指示された通信品質を各装置が満足するように転送機能を実現するように構成されている。

【0005】 さてこうした既存の通信網では、特にIP などのレイヤ3の転送が重要視されておりルーティングと呼ばれるレイヤ4を重点的に転送処理できる装置が網内に数多く配置されている。

【0006】 これらルーティング装置ではレイヤ3のIP を終端し、そのデータグラムから導出される宛先IP アドレスから装置内にあらかじめ蓄積された経路情報から転送すべき経路を決定することによりデータグラムの転送を行なっている。この際、データグラムが導出される物理レイヤ4の処理は経路から容易に導き出される1 経路を選択しデータグラムを該インフラフェースから転送する処理を行なっている。

【0007】 なお、アプリケーションごとの通信品質を保証し、かつルーティングを用いることなく異なるサブネットワーク間でデータ転送を可能とするネットワークサーバが、特開9-116560 号公報に開示されている。

【0008】

【発明が解決しようとする課題】 上述した従来のルーティング装置では、データグラムの通信属性に応じたコネクション品質により最適な通信品質を決定したデータグラムを転送することができない。その理由は、データグラムから導出される宛先IP アドレスから装置内にあらかじめ蓄積された経路情報から転送すべき経路を決定することに

TPヘッダに含まれるLocationによりHTTPデータのおかれているURI、HTTPヘッダに含まれるForwardedによりデータの転送先URI及び転送元ポート番号、HTTPヘッダに含まれるContent-Baseによりデータのbase URI、HTTPヘッダに含まれるContent-LocationによりHTTPデータの存在するURI、HTTPヘッダに含まれるMethodによりユーザプログラムからのHTTPデータ要求方法の少なくとも1を検査することを特徴とする。

[00032] 請求項12の本発明の通信品質制御装置では、前記属性識別手段が、前記識別情報として、受信データグラムのHTTPヘッダに含まれるMIME-VersionによりデータのMIME (Multi purpose Internet Mail Extensions) のVersion、HTTPヘッダに含まれるAcceptによりユーザプログラムの許可するメディア属性、HTTPヘッダに含まれるAccept-Charsetによりユーザプログラムの許可する文字セット、HTTPヘッダに含まれるAccept-Encodingによりユーザプログラムの許可するデータのコーデック方法、HTTPヘッダに含まれるAccept-Languageによりユーザプログラムの許可するデータの言語、HTTPヘッダに含まれるContent-Encodingによりデータのエンコード方法、HTTPヘッダに含まれるCookieにより言語として、受信データグラムのHTTPヘッダに含まれるStatus Codeによりユーザプログラムからの要求に対するサーバの応答内容、HTTPヘッダに含まれるWWW-Authenticateによりサーバの要求する認証情報、HTTPヘッダに含まれるProxy-Authorizationによりサーバの認証情報の少なくとも1を検査することを特徴とする。

[00033] 請求項13の本発明の通信品質制御装置では、前記属性識別手段が、前記識別情報として、受信データグラムのHTTPヘッダに含まれるStatus Codeによりユーザプログラムからの要求に対するサーバの応答内容、HTTPヘッダに含まれるWWW-Authenticateによりサーバの要求する認証情報、HTTPヘッダに含まれるProxy-Authorizationによりサーバの認証情報の少なくとも1を検査することを特徴とする。

[00034] 請求項14の本発明の通信品質制御装置では、前記属性識別手段が、前記識別情報として、受信データグラムのHTTPヘッダに含まれるAllowによりデータの許可するMethod、HTTPヘッダに含まれるAccept-Rangeによりサーバの許可するRange要求方法、HTTPヘッダに含まれるHostによりHTTPデータを要求されるホスト及びそのポート番号、HTTPヘッダに含まれるIf-RangeによりHTTPデータの取得条件、HTTPヘッダに含まれるPublicによりサーバの許可するMethod、HTTPヘッダに含まれるRangeに

よりユーザプログラムの要求しているHTTPデータのRangeの少なくとも1を検査することを特徴とする。

[00035] 請求項15の本発明の通信品質制御装置では、前記属性識別手段が、前記識別情報として、受信データグラムのHTTPヘッダに含まれるContent-Lengthによりデータのデータ長、HTTPヘッダに含まれるConnectionによりデータのデータの接続の状態、HTTPヘッダに含まれるWarningによりユーザプログラムの要求に対するサーバの応答情報、HTTPヘッダに含まれるRetry-Afterにより要求されたHTTPデータを取得可能な日時、HTTPヘッダに含まれるViaによりパケットを中継してきたプロキシサーバまたはゲートウェイのプロトコルVersion及びホスト名及び使用ソフトウェア名、HTTPヘッダに含まれるTransfer-Encodingによりデータのデータのコーデック方法の少なくとも1を検査することを特徴とする。

[00036] 請求項16の本発明の通信品質制御装置によれば、レイヤ3をIPとし、レイヤ4をTCPまたはUDP (User Datagram Protocol) として、前記属性識別手段は、前記データグラムのIPヘッダのプロトコル番号またはIPヘッダの次の値を検査し、レイヤ4がTCPまたはUDPであることを認識するとともに、識別情報として受信データのTCPヘッダまたはUDPヘッダに含まれる一つまたは複数の識別情報を検査し、前記通信品質決定手段は、前記データグラムがプロトコル終端装置に転送された場合には、前記データグラムより抽出されたコネクションに最適なレイヤ3以下のコネクションの品質を決定し、コネクションの品質に基づくデータグラム転送処理を行なうことにより、送信すべきデータグラムのコネクション品質を変えて制御することを特徴とする。

[00037] 請求項17の本発明の通信品質制御装置では、前記属性識別手段は、前記識別情報として、受信データグラムのUDPヘッダに含まれるchecksumフィールドを検査することを特徴とする。

[00038] 請求項18の本発明の通信品質制御装置では、レイヤ3をIPとし、レイヤ4をTCPまたはUDPとし、レイヤ5をDNSまたはFTPまたはSNMPとして、前記属性識別手段は、前記データグラムのIPヘッダのプロトコル番号、または該プロトコル番号と前記データグラムのTCPまたはUDPデータのIPヘッダの次のヘッダ値、または該ヘッダ値と前記データグラムのTCPまたはUDPプロトコルヘッダ内のポートアドレスを検査し、レイヤ5がDNSまたはFTPまたはSNMPであることを認識するとともに、識別情報として受信データのDNSメッセージ、TCPまたはU

ジョン品質を用いてデータグラムの転送が可能となるものである。

[00023] 請求項3の本発明の通信品質制御装置では、前記属性識別手段が、受信されたデータグラムより、前記レイヤ情報を識別すると共に、前記データグラムのコネクション識別情報よりコネクションの状態を識別してコネクション情報として前記通信品質決定手段に出力し、かつ前記データグラムの転送経路を決定し転送先経路情報として前記通信品質決定手段に出力し、前記通信品質決定手段は、前記属性情報に対処するコネクションの品質情報を決定し、前記コネクション情報と、前記コネクションの品質情報と、前記転送先経路情報により、データグラムを送信する通信品質を決定することを特徴とする。

[00024] 請求項4の本発明の通信品質制御装置では、前記属性識別手段は、識別したコネクションの状態から、レイヤ4以上の属性を検出する必要があると判断した場合に、前記レイヤ情報と、前記データグラムの一部または全部に基づいて、通信の属性情報を取り出すことを特徴とする。

[00025] 請求項5の本発明の通信品質制御装置では、前記通信データグラム転送装置が、コネクション情報と通信品質を組にして記録したコネクション通信品質テーブルを備え、前記通信品質決定手段は、前記コネクション情報と前記転送先経路情報、またはコネクション品質情報が入力した場合に、前記データグラムが前記コネクション通信品質テーブルによる管理が必要かどうかを判断し、管理が必要がある場合、前記コネクション通信品質テーブルに同一のコネクションが存在するかを検査し、同一のコネクションが存在する場合、コネクション通信品質テーブルを参照して通信品質を決定し、存在しない場合、前記コネクション情報と、前記コネクションの品質情報と、前記転送先経路情報により通信品質を決定しかつコネクション情報と通信品質を組にして前記コネクション通信品質テーブルに記録し、管理の必要がない場合、前記コネクション情報と前記転送先経路情報により通信品質を決定することを特徴とする。

[00026] 請求項6の本発明の通信品質制御装置では、前記属性情報に対処する前記コネクション品質情報を格納するデータベースを備え、前記通信品質決定手段は、前記データベースを参照し、前記属性情報に基づいて前記コネクション品質情報を決定することを特徴とする。

[00027] 請求項7の本発明の通信品質制御装置では、レイヤ3をIPとし、レイヤ4をTCPとし、レイヤ5をHTTPとし、前記属性識別手段は、前記データグラムのIPヘッダのプロトコル番号、または該プロトコル番号と前記データグラムのTCPプロトコルヘッダ内のポートアドレス、または前記データグラムのIPヘ

ッダの次のヘッダ値、または該ヘッダ値と前記データグラムのTCPプロトコルヘッダ内のポートアドレスとを検査し、レイヤ5がHTTPであることを認識するとともに受信データグラムのTCPヘッダまたは、TCPヘッダ及びHTTPメッセージに含まれる一つまたは複数の識別情報を検査し、前記通信品質決定手段は、前記データグラムがプロトコル終端装置に転送された場合には、前記データグラムのコネクションの品質を決定し、コネクションの品質に基づくデータグラム転送処理を行なうことにより、送信すべきデータグラムのコネクション品質を変えて制御することを特徴とする。

[00028] 請求項8の本発明の通信品質制御装置では、前記属性識別手段が、前記識別情報として、受信データグラムのHTTPヘッダに含まれるContent-typeによりデータのメディア属性、HTTPヘッダに含まれるFromフィールドによりデータグラムを送出したユーザの電子メールアドレス、HTTPヘッダに含まれるUser-Agentによりデータグラムを作成したユーザプログラムの名及びVersion、HTTPヘッダに含まれるServerによりデータグラムを作成したサーバソフトウェア名及びVersionの少なくとも1を検査することを特徴とする。

[00029] 請求項9の本発明の通信品質制御装置では、前記属性識別手段が、前記識別情報として、受信データグラムのHTTPヘッダに含まれるDateによりデータグラムの作成日時、HTTPヘッダに含まれるAuthorizationによりデータのデータの認証情報、当該認証情報の暗号化方法、HTTPヘッダに含まれるExpiresによりデータグラムの有効時間の少なくとも1を検査することを特徴とする。

[00030] 請求項10の本発明の通信品質制御装置では、前記属性識別手段が、前記識別情報として、受信データグラムのHTTPヘッダに含まれるPragmaによりデータの要求事項、HTTPヘッダに含まれるCache-Controlによりデータグラムのキャッシュ制御情報、HTTPヘッダに含まれるIf-Modified-SinceによりMethodの実行条件、HTTPヘッダに含まれるIf-UnauthorizedによりMethodの実行条件、HTTPヘッダに含まれるRequest-Line) 内のリクエストURIによりクライアントの要求しているURI、HTTPヘッダに含まれるLast-ModifiedによりHTTPデータの最終更新日時の少なくとも1を検査することを特徴とする。

[00031] 請求項11の本発明の通信品質制御装置では、前記属性識別手段が、前記識別情報として、受信データグラムのHTTPヘッダに含まれるRefererによりHTTPデータの参照元URI (Uniform Resource Identifiers)、HT

装置1とから構成されている。

【0051】 ネットワーク終端装置2a、2b、2c、・・・2nは、受信したデータグラムに関しデータネットワークのフロトコルレイヤの終端を行なう。データネットワークのフロトコルレイヤとは、具体的に、M-AC層やATM層等である。フロトコル終端装置3aは、ネットワーク終端装置2aより転送されるデータグラムの通信の品質に基づき1P層などのレイヤ3以下を終端する。同時にフロトコル終端装置3b、3c、・・・3nは、ネットワーク終端装置2b、2c、・・・2nより転送されるデータグラムの通信の品質に基づき1P層などのレイヤ3以下を終端する。

【0052】 通信データグラム転送装置1は、フロトコル終端装置3a、3b、3c、・・・3nより受信したデータグラムに含まれるフロトコルレイヤ4、5、6、7の各々またはいずれかのレイヤの情報から導出される通信の属性に対応するコネクションの品質情報に従ってフロトコル終端装置4a、4b、4c、・・・4nの何れかにデータグラムを転送する。また、通信データグラム転送装置1は、該コネクションの品質情報に従ってデータグラムを送信する通信品質を決定し、該フロトコル終端装置4a、4b、4c、・・・4nに対して通知する。

【0053】 フロトコル終端装置4aは、通信データグラム転送装置1よりデータグラムとデータグラムを送信する通信品質を受信すると、通知された通信品質に基づきフロトコルレイヤ3以下の設定を行ない、ネットワーク終端装置5aへ転送し、ネットワーク終端装置5aは、該データグラムを外部ネットワークへ転送する。同様に、フロトコル終端装置4b、4c、・・・4nは、通信データグラム転送装置1よりデータグラムとデータグラムを送信する通信品質を受信すると、通知された通信品質に基づきフロトコルレイヤ3以下の設定を行ない、ネットワーク終端装置5b、5c、・・・5nへ転送し、ネットワーク終端装置5b、5c、・・・5nは、該データグラムを外部ネットワークへ転送する。

【0054】 通信品質制御装置1は、論理的には、複数のフロトコル終端装置とにより構成されるが、物理的には、同一のハードウェアで構成されているとも良い。同様に、通信品質制御装置1は、論理的には、複数のネットワーク終端装置とにより構成されるが、物理的には、各ネットワーク終端装置のすべてまたはそのいくつかは同一のハードウェアで構成されているとも良い。具体例をあげると、ATMにおける通信では、VP (Virtual Path) 毎に仮想的な宛先とのパスが与えられるため、論理的には、それぞれのVPを一つのネットワーク終端装置により終端するが、物理的には一つの物理回路を終端する終端装置が複数のVPを終端している場合が考えられる。

【0055】 送信側のフロトコル終端装置3a、3b、3c、・・・3nと受信側のフロトコル終端装置4a、4b、4c、・・・4nは、論理的には、送信、受信と別の機能を有するが、物理的にはそれぞれが同一のハードウェアで構成されているとも良い。同様に、送信側のネットワーク終端装置2a、2b、2c、・・・2nと受信側のネットワーク終端装置5a、5b、5c、・・・5nは、論理的には、送信、受信と別の機能を有するが、物理的にはそれぞれが同一のハードウェアで構成されているとも良い。

【0056】 図2は、上記した通信データグラム転送装置1の構成例を示すブロック図である。

【0057】 通信データグラム転送装置1は、入力キュー管理部11、出力キュー管理部12、レイヤ識別部13、属性抽出部14、通信品質決定部15、経路決定部16、コネクション通信品質管理部17、QoSデータベース150、経路テーブル160、コネクション通信品質テーブル170より構成される。

【0058】 入力キュー管理部11は、各フロトコル終端装置3a、3b、3c、・・・3nよりデータグラムが入力されると優先度の高いデータグラムを選択すると共に、該データグラム(D)をレイヤ識別部13と出力キュー管理部12に対して出力する。

【0059】 レイヤ識別部13は、図3のフローチャートに基づいて動作する。まず、レイヤ識別部13は、入力された該データグラム(D)に関し、各レイヤの識別を行なう(ステップ301)。具体的には、レイヤ3が1Pである場合、1Pヘッダのバージョンにより1Pフロトコルのバージョンを認識し、レイヤ3により1Pである場合、1Pヘッダのフロトコル番号、または前記フロトコル番号と該データグラムのTCPまたはUDPフロトコルヘッダのポート番号を参照することによりアプリケーションを識別する。また、レイヤ3が1Pv6である場合、1Pヘッダの次ヘッダ値、または前記次ヘッダ値とTCPまたはUDPフロトコルヘッダのポート番号を参照することによりアプリケーションを識別する。

【0060】 レイヤ識別部13は、入力された該データグラム(D)より通信品質を決定するトラフィックの単位となるコネクションの識別を行なう(ステップ302)。具体的には、レイヤ3が1Pでありレイヤ4がTCPまたはUDPである場合、1Pヘッダの送信1Pアドレス、宛先1PアドレスとTCPまたはUDPヘッダの送信ポート番号、宛先ポート番号の組からなるコネクション識別情報によりコネクションを識別する。

【0061】 レイヤ識別部13は、前記コネクション識別情報により識別したコネクションにおいて、該コネクションの状態を識別し、コネクション通信品質管理部17に対して、コネクション情報(C)として、コネクションの識別情報とコネクションの状態情報を出力する。

DPヘッダとDNSメッセージ、FTPメッセージ、UDPヘッダとFTPメッセージ、SNMPメッセージ、またはUDPヘッダとSNMPメッセージの何れかに含まれる一つまたは複数の識別情報を抽出し、前記通信品質決定手段は、前記データグラムがフロトコル終端装置に転送された場合に、前記データグラムより抽出されたコネクションに最適なレイヤ3以下のコネクションの品質を決定し、コネクションの品質に基づくデータグラム転送処理を行なうことにより、送信すべきデータグラムのコネクション品質を変えて制御することと特徴とする。

【0039】 請求項19の本発明の通信品質制御装置では、前記属性識別手段は、前記識別情報として、受信データグラムのDNSメッセージにquery typeが存在するかどうかを検査することと特徴とする。

【0040】 請求項20の本発明の通信品質制御装置では、前記属性識別手段は、前記識別情報として、受信データグラムのFTPメッセージに含まれるopcodeを検査することと特徴とする。

【0041】 請求項21の本発明の通信品質制御装置では、前記属性識別手段は、前記識別情報として、受信データグラムのSNMPメッセージに含まれるPDUタイプを検査することと特徴とする。

【0042】 請求項22の本発明の通信品質制御装置では、レイヤ3を1Pとし、レイヤ4をTCPとし、レイヤ5をFTPまたはSMTPまたはとして、前記属性識別手段は、前記データグラムの1Pヘッダのフロトコル番号、または該フロトコル番号と前記データグラムのTCPヘッダのポートアドレス、または該ポートアドレスと前記データグラムのUDPヘッダのポートアドレスとを抽出し、レイヤ5がFTPまたはSMTPであることと特徴するとともに、識別情報として受信データのFTP Command、FTP Reply、TCPヘッダとFTP CommandまたはFTP Reply、SMTP Command、SMTP Reply Code、SMTPヘッダ、TCPヘッダとSMTP CommandまたはSMTP Reply CodeまたはSMTPヘッダの何れかに含まれる一つまたは複数の識別情報を抽出し、前記通信品質決定手段は、前記データグラムがフロトコル終端装置に転送された場合に、前記データグラムより抽出されたコネクションに最適なレイヤ3以下のコネクションの品質を決定し、コネクションの品質に基づくデータグラムのコネクション品質を変えて制御することと特徴とする。

【0043】 請求項23の本発明の通信品質制御装置では、転送の物理レイヤをATM転送方式とし、コネクション品質に基づきデータグラム転送処理としてATMの各々のコネクション品質に別々のVC (Virtual Circuit) を割り当ててデータグラムの転送を行ない、各々のVCはコネクション品質に応じた通信品質制御パラメータが設定されていることにより、データグラムから抽出されるメタデータの属性に応じた転送が行なわれることを特徴とする。

【0044】 請求項24の本発明の通信品質制御装置では、前記通信品質決定手段は、前記通信品質に加えて、コネクション設定のためのコネクション設定メッセージに応じたコネクション設定ロバステネスを選択して設定することと特徴とする。

【0045】 請求項25の本発明の通信品質制御装置によれば、前記通信品質決定手段は、前記属性情報により、前記コネクションの通信品質として、最適な帯域幅に関する制御パラメータ、最大遅延時間や遅延時間変動量を含む遅延時間に関する最適な制御パラメータ、バッファ量を含むデータ喪失に関する最適な制御パラメータ、最適な現金情報に関する制御パラメータのうち少なくとも1つの制御パラメータを決定することと特徴とする。

【0046】 請求項26の本発明の通信品質制御装置では、前記通信品質決定手段は、前記コネクションの通信品質に基づき、最適なデータグラムの転送先、最適なデータグラムの転送経路の少なくとも一方を決定することと特徴とする。

【0047】 請求項27の本発明の通信品質制御装置では、前記通信品質決定手段は、前記コネクションの通信品質に基づいて、必要に応じて専用の物理回路を該コネクションによって使用し、前記データグラムを符号化または復号化して転送し、データグラム内の不要な情報を削除し、圧縮してデータグラムのサイズを削減し、データグラムのトンネリングを行なうことと特徴とする。

【0048】 請求項28の本発明の通信品質制御装置では、前記通信品質決定手段は、前記属性情報によりコネクションの通信品質としてコネクション設定優先度またはコネクション転送優先度を設定し、該コネクション設定優先度の高いコネクションのコネクション設定処理を優先し、またはコネクション転送優先度の高いコネクションのデータグラムの転送を優先させることを特徴とする。

【0049】

【発明の実施の形態】

【構成の説明】 次に、本発明の実施の形態について図面を参照して詳細に説明する。

【0050】 図1は本発明の第1の実施の形態を示す通信品質制御装置6のブロック図である。本実施の形態の通信品質制御装置6は、複数のネットワーク終端装置2a、2b、2c、・・・2n及び5a、5b、5c、・・・5nとフロトコル終端装置3a、3b、3c、・・・3n及び4a、4b、4c、4nの組、そして、各々のフロトコル終端装置を接続する通信データグラム転送

る。コネクシオン品質情報 (S) が入力されない場合には、当該データグラムについてコネクシオン-通信品質 (Q) と通信品質 (Q) を組にして記録しておく。一度、コネクシオン品質 (S) に対処する通信品質 (Q) が決定すると、レイヤ識別部 13 より入力されるコネクシオン-通信品質 (Q) と経路決定部 16 より入力される転送性経路 (R 2) により、通信品質 (Q) を決定する。

【0077】また、コネクシオン品質情報 (S) が入力された場合であっても、当該データグラムについてコネクシオン-通信品質 (Q) と通信品質 (Q) を組にして記録しておく。一度、コネクシオン品質 (S) に対処する通信品質 (Q) が決定すると、レイヤ識別部 13 より入力されるコネクシオン-通信品質 (Q) と経路決定部 16 より入力される転送性経路 (R 2) により、通信品質 (Q) を決定する。

【0078】HTTPセッションを含むコネクシオン-通信品質 (S) が決定された場合、レイヤ識別部 13 より入力されるコネクシオン-通信品質 (Q) と通信品質 (Q) を組にして記録しておく。一度、コネクシオン品質 (S) に対処する通信品質 (Q) が決定すると、レイヤ識別部 13 より入力されるコネクシオン-通信品質 (Q) と経路決定部 16 より入力される転送性経路 (R 2) により、通信品質 (Q) を決定する。

【0079】コネクシオン-通信品質管理 17 は、コネクシオン-通信品質 (S) を組にして記録しておく。一度、コネクシオン品質 (S) に対処する通信品質 (Q) が決定すると、レイヤ識別部 13 より入力されるコネクシオン-通信品質 (Q) と通信品質 (Q) を組にして記録しておく。一度、コネクシオン品質 (S) に対処する通信品質 (Q) が決定すると、レイヤ識別部 13 より入力されるコネクシオン-通信品質 (Q) と経路決定部 16 より入力される転送性経路 (R 2) により、通信品質 (Q) を決定する。

【0080】出力キュー管理 12 は、入力キュー管理 11 より入力されたデータグラム (D) に関して、コネクシオン-通信品質管理 17 より入力される通信品質 (Q) に基づき、最適なプロトコル経路 (R 2) を決定する。一度、コネクシオン品質 (S) に対処する通信品質 (Q) が決定すると、レイヤ識別部 13 より入力されるコネクシオン-通信品質 (Q) と経路決定部 16 より入力される転送性経路 (R 2) により、通信品質 (Q) を決定する。

【0081】レイヤ 3 が IP であり、レイヤ 4 が TCP であり、レイヤ 5 が HTTP である場合に関して、本発明の実施形態における動作に関して説明する。

【0082】コネクシオン品質情報 (S) が入力されない場合とレイヤ 4 以上のデータグラム参照の必要のないデータグラムの場合、データグラムの動作では、コネクシオン-通信品質管理 17 は、コネクシオン品質情報 (C) と転送性経路 (R) よりデータグラム (D) を転送するための通信品質 (Q) を決定する。

【0083】図 5 に示すように、HTTPセッション (H0) はいくつかの IP データグラム (H1, H2, H3, ...) に分割されてネットワーク上に転送されており、HTTPセッションにおいて通信の属性を規定すると考えられる HTTP ヘッダを含んだデータグラムは、先頭のデータグラム (H1) である。

【0084】よって、レイヤ識別部 13 は、TCP ヘッダのポートを監視することにより、先頭のデータグラム (H1) を受信時に、コネクシオン確立後の最初のデータグラムであることを認識する。そして、レイヤ識別部 13 は、属性抽出部 14 に対して、レイヤ 4 が HTTP であるというレイヤ情報 (L) を出力する。また、属性抽出部 14 は、データグラム (H1) 内の HTTP ヘッダより通信品質を決定するために必要な属性を抽出し、通信品質決定部 15 に対して属性情報 (P) を出力する。

【0085】通信品質決定部 15 では、属性抽出部 14 より入力された属性情報 (P) を基に QoS データベース 150 を検索し、コネクシオン品質 (S) を決定し、コネクシオン-通信品質管理 17 に対して出力する。

【0086】コネクシオン-通信品質管理 17 は、データグラム (H1) がコネクシオン-通信品質管理 17 より入力されたコネクシオン品質 (S) と経路決定部 16 より入力された転送性経路 (R) を基に、データグラム (H1) の通信品質 (Q) を決定し出力キュー管理 12 へ転送する。

【0087】コネクシオン-通信品質管理 17 は、コネクシオン-通信品質 (C) と通信品質 (Q) の組をコネクシオン-通信品質管理 17 に対して出力する。

【0088】次に、データグラム (H2) を受信した場合、コネクシオン-通信品質管理 17 は、レイヤ識別部 13 より入力されるコネクシオン品質情報 (C) を基に、コネクシオン-通信品質管理 17 の検索を行ない、データグラム (H1) と同一の通信品質においてデータグラムの転送が行なわれる。

【0089】データグラム (H3) 以降においても、同様データグラム (H1) と同一の通信品質においてデータグラムの転送が行なわれる。

【0090】本発明の通信データグラム転送装置 1 は、あくまでもデータグラムのレイヤ 3 以下を転送しデータグラムの転送を行なうため、既存のルーティングと同様に高速であるが、必要に応じてレイヤ 4 以上の通信属性を検査し、該通信属性に対応する最適な通信品質においてデータグラムの転送を行うことが可能である。

【0091】

【実施例 1】次に、通信データグラム転送装置 1 の実施例として、転送の物理レイヤを ATM 転送方式とし、レイヤ 3 が IP v4、レイヤ 4 が TCP、レイヤ 5 が HTTP であるデータグラムの転送を行なう場合に関して、

(スレッズ 303)。コネクシオンの状態を識別すると、具体的には、レイヤ 4 が TCP である場合、TCP ヘッダ内部のポートにおいて、SYN フラグが立っていることにより TCP のコネクシオンの確立が行なわれていることを認識し、FIN フラグが立っていることにより、TCP のコネクシオンが終了することを認識する。

【0062】レイヤ識別部 13 は、経路決定部 15 に対して、経路を決定するために必要な属性 (A) を出力する (スレッズ 304)。

【0063】そして、レイヤ識別部 13 は、前記識別したコネクシオンの状態をもとに、属性抽出部 14 においてレイヤ 4 以上の属性を抽出する必要があるかどうかを判断する (スレッズ 305)。

【0064】レイヤ 4 以上の属性を抽出する必要があると判断した場合、属性抽出部 14 に対して、該データグラムの前記レイヤ情報 (L) と属性抽出部 14 が各レイヤから属性を抽出するために必要なデータグラムの一部もしくは全部 (DP) を出力する (スレッズ 306)。

【0065】属性抽出部 14 は、レイヤ識別部 13 から入力される前記レイヤ情報 (L) を基に入力されたデータグラムの一部もしくは全部 (DP) から通信の属性情報の抽出を行ない、抽出された該通信の属性情報 (P) を通信品質決定部 15 へ出力する。

【0066】属性抽出部 14 では、データグラムのレイヤ 4、5、6、7 の各々またはいずれかのレイヤの属性に合致する識別情報の抽出を行なうが、コネクシオンの品質を規定するために必要であれば、レイヤ 3 以下の情報に際しても抽出を行なうものとする。

【0067】通信品質決定部 15 は、QoS データベース 150 を参照し、属性抽出部 14 より入力された通信の属性情報 (P) に対応するコネクシオン品質情報 (Q) を検索し、コネクシオン-通信品質管理 17 へ出力する。

【0068】経路決定部 16 は、レイヤ識別部 13 より入力される前記経路を決定するために必要な属性 (A) を基に、経路データグラム 160 の検索を行ない、データグラムの転送性経路を決定し、コネクシオン-通信品質管理 17 へ該データグラムの転送性経路情報 (R) を出力する。

【0069】具体的にはレイヤ 3 である場合、前記経路を決定するために必要な属性 (A) は、宛先 IP アドレスであり、宛先 IP アドレスをキーとして、宛先 IP アドレスの属する IP サブネットワークアドレスまたは宛先 IP アドレス自身を検索し、該 IP サブネットワ

ークアドレスに属する次に送信すべき装置の IP アドレスまたは VPI (Virtual Path Identifier) 等を決定する。

【0070】コネクシオン-通信品質管理 17 は、図 4 のフローチャートに基づいて動作する。まず、コネクシオン-通信品質管理 17 は、レイヤ識別部 13 からのコネクシオン品質情報 (C) 及び経路決定部 16 からの転送性経路情報 (R) と、または通信品質決定部 15 からのコネクシオン品質情報 (S) を入力する (スレッズ 401)。

【0071】コネクシオン-通信品質管理 17 は、レイヤ識別部 13 より入力されるコネクシオン品質情報 (C) より、コネクシオン-通信品質管理 17 において管理する必要があるデータグラム (D) か、または当該データグラムへの記録の必要があるデータグラム (D) かを判断する (スレッズ 402)。

【0072】コネクシオン-通信品質管理 17 において管理する必要があるデータグラム (D) である場合には、レイヤ識別部 13 より入力されるコネクシオン品質情報 (C) と経路決定部 16 より入力される転送性経路情報 (R) により、通信品質 (Q) を決定し、出力キュー管理 12 (2) に対して出力する (スレッズ 403)。

【0073】コネクシオン-通信品質管理 17 において管理する必要があるデータグラム (D) である場合、コネクシオン-通信品質管理 17 は、コネクシオン-通信品質管理 17 170 の検索を行ない、同一のコネクシオンが存在するかどうかを判断する (スレッズ 404)。

【0074】コネクシオン-通信品質管理 17 170 の検索により同一コネクシオンが存在する場合は、コネクシオン-通信品質管理 17 170 を参照して、通信品質 (Q) を決定する (スレッズ 405)。

【0075】コネクシオン-通信品質管理 17 170 の検索により同一コネクシオンが存在しない場合は、通信品質決定部 15 から入力されるコネクシオンの品質情報 (S)、レイヤ識別部 13 より入力されるコネクシオン品質情報 (C)、経路決定部 16 より入力される転送性経路情報 (R) により、データグラム (D) を転送するため通信品質 (Q) を決定し、出力キュー管理 12 (2) に対して出力する (スレッズ 406)。

【0076】コネクシオン品質情報 (S) が入力されるのは、レイヤ識別部 13 においてレイヤ 4 以上の属性を識別する必要があると判断された場合のみであ

うに、レイヤ4以上より識別された属性情報だけでなく、必要に応じてレイヤ3以下の属性情報をも利用することによりコネクションの品質を決定する。

[0104] 転送先VPI (42) は、データグラムの転送先を決定する。

[0105] 基本的に、データグラムの転送先は、経路決定部16において、経路テーブル160を参照することにより決定する。図9に経路テーブル160の例を示す。図9を参照すると、経路テーブル160は、宛先IPアドレス (43) と転送先VPI (36-1) の組み合わせで構成されている。経路決定部16は、レイヤ識別部13より入力される宛先IPアドレス (41) が経路テーブル160内のどのサブネットワークアドレス (43) に属するかを検索し、対応する転送先VPI (36-1) を決定する。

[0106] 拡張QOSテーブル150Bの項番6では、宛先IPアドレス (41) がIPアドレス1であり、Content-Type (21) がApplication/x-newtypeというあるアプリケーションを使用している場合に、転送先VPI (42) をVPI5に設定する。よって、コネクション通信品質管理部17は、通信品質決定部15より入力されるコネクション品質 (S) に転送先VPI (36-2) が設定されている場合は、経路決定部より出力される転送先VPI (36-1) よりも優先する。このように通信品質決定部15においても転送先VPI (36) の決定を可能にし、コネクション通信品質管理部17において、経路決定部16で決定する転送先VPI (36-1) よりも通信品質決定部15で決定する転送先VPI (36-2) を優先する機能を有することにより、使用するアプリケーションの種類や、使用するユーザにより転送経路または転送先を変更することが可能である。

[0107] 付加品質 (35) は、コネクション品質としてセキュリティ品質に応じたデータ転送を確保するためのデータグラムの暗号化方法を規定する。図8の項番7では、IPアドレス4からIPアドレス3へのテキストデータの通信では、L2TP (Layer 2 Tunneling Protocol) を用いてデータグラムの暗号化、及びトンネリングを行なうことを示している。

[0108] 図8の拡張QOSテーブル150Bでは送信元IP (42)、宛先IP (41) が記入されたIPアドレスと一致するかを判定することにより、コネクション品質を決定するが、図9の経路テーブルと同様に、IPサブネットワークアドレスを記入し、送信元IP (42) 及び宛先IP (41) がIPサブネットワークアドレスに属するかどうかを判定することにより、サブネットワークアドレスの品質を決定する通用も可能である。

[0109] コネクション通信品質管理部17では、通信品質決定部15から入力されるコネクション品質

(S) である、遅延優先度 (31)、損失優先度 (32)、帯域 (33)、コネクション優先度 (34)、付加品質 (35) と、転送先VPI (36-2) と、経路決定部16から入力される転送先VPI (36-1) をもとにデータグラムを送信するための通信品質 (Q) としてVPIとVCIを決定し、出力キュー管理部12へ出力する。

[0110] そして、出力キュー管理部12では、VPIにより定められるバスとVCIにより定められる品質により最適フロートコル排他管理を選択しデータグラムを転送する。

[0111] 出力キュー管理部12では、遅延優先度 (31) の高いデータグラムを優先的に処理する。

[0112] 出力キュー管理部12では、損失優先度 (32) の高いデータグラムに対して多くのバッファ量を用意することにより、輻射発生時に損失優先度 (32) の低いデータグラムから放棄されるような制御を行なう。

[0113] コネクション通信品質管理部17では、新たなコネクションを抽出した場合、もしくは、コネクションの通信品質が変更される場合、必要に応じて他のATM装置の間にVC (Virtual Circuit) の設定を行なう。コネクション優先度 (34) の高いデータグラムは、VC (Virtual Circuit) を割り当てる際に、より優先的にコネクションの設定が行なわれる。

[0114] 具体的には、以下のように設定を行なう。

[0115] (1) コネクション優先度 (34) の高いデータグラムとコネクション優先度 (34) の低いデータグラムの両方のVC設定を行なう必要がある場合、コネクション優先度 (34) の高いコネクションのVC設定を先にこなう。

[0116] (2) コネクション優先度 (34) の高いデータグラムのVC設定ができない場合、コネクション優先度 (34) の低いVCを開放して、コネクション優先度 (34) の高いデータグラムのVC設定を行なう。

[0117] (3) VCIリソースが少なくなってきた場合には、リソースを使い切る前に、コネクション優先度 (34) の低いVCを開放する。

[0118] 転送先VPI (36) のうちいくつかのVPIに関しては、専用の物理回線を使いバスを設定することより、セキュリティ品質を高めることが可能である。例えば、転送先VPI (36-2) のVPI6を専用の物理回線として割り当てることにより、図8の拡張QOSテーブル150Bの項番7において、送信元IP (42) がIPアドレス4で宛先IP (41) がIPアドレス3であり、Content-Type (21) が"text"であるデータに関して、専用の物理回線が割り当てられるため、セキュリティ品質の高いデータグラムの転送が可能である。

属性抽出部13において抽出する属性情報 (P) の内容、及び、通信品質決定部14において属性情報 (P) より決定するコネクション品質 (S) の内容、及び、コネクション品質 (S) によりどのような通信品質を提供するかに関して、より具体的に説明する。

[0092] HTTPセッションの最初のデータグラムを受信した際、レイヤ識別部13は、IPヘッダのフロート番号が6であることよりレイヤ4がTCPであることを認識し、TCPヘッダのポート番号が80であることを認識し、TCPがHTTPであることを認識し、レイヤ情報として属性抽出部14へ出力する。

[0093] 属性抽出部14は、レイヤ5がHTTPであることから、HTTPヘッダにContent-Type (21)、Server (22)、User-Agent (23)、From (24) が存在するかのチェックを行ない、存在する場合その属性値と共に、通信品質決定部15へ出力する。

[0094] RFC (Request For Comment) 1521で規定されているContent-Type (21) は、メディア属性を示し、基本タイプ/サブタイプの組で表現される。例えば、基本タイプが"image"の場合は画像を、"video"の場合は動画、"audio"の場合は音声、"text"の場合はテキストデータであることが分かる。Server (23) は、HTTPによる要求に答えるサーバのプログラム名、バージョンを示す。User-Agent (22) は、HTTPによりデータを要求するユーザの使用するクライアントプログラムのバージョンを示す。From (24) は、HTTPによりデータを要求するユーザの電子メールアドレスを使用する。

[0095] 属性抽出部14は、コネクション品質を決定するための属性値として、HTTPヘッダから抽出する属性値以外に、IPヘッダより宛先IPアドレス (41)、送信元IPアドレス (42) を抽出し、通信品質決定部15へ出力する。

[0096] 通信品質決定部15は、属性抽出部14より入力される各属性値を基に、QOSデータベース150の検索を行なう。本実施例では、QOSデータベース150として、図7の基本QOSテーブル150Aと、図8の拡張QOSテーブル150Bを用いる。

[0097] 図7の基本QOSテーブル150Aを参照すると、Content-Type (21) の属性値を基に、遅延優先度 (31)、損失優先度 (32)、帯域 (33)、コネクション優先度 (34) が設定されている。

[0098] 遅延優先度 (31) は、値が大きいものは優先的に転送されることを意味する。損失優先度 (32) は、値が大きいものは輻射発生時に優先的に放棄される。コネクション優先度 (34) は、値が大きいものは優先的にコネクションを設定することを意味する。

[0099] 図7の例では、Content-Type (21) の値により、メディア属性が画像であるか、音声であるか、動画であるか、他のデータであるかの判断を行ない、音声や動画の場合には、他のメディアに比べ遅延優先度を高く設定することによりリアルタイムでの通信が可能となるようにしている。また、音声、画像、動画の各メディアは、その他のデータアプリケーションに比べ多少のデータ損失が許されるため、損失優先度 (32) が小さく設定されている。

[0100] 図8の拡張QOSテーブル150Bの例を参照すると、宛先IP (41)、送信元IP (42)、Content-Type (21)、Server (22)、User-Agent (23)、From (24) を基に、遅延優先度 (31)、損失優先度 (32)、帯域 (33)、コネクション優先度 (34)、付加品質 (35)、転送先VPI (36-2) を決定する。

[0101] 遅延優先度 (31)、損失優先度 (32)、帯域 (33)、コネクション優先度 (34) の定義は、前記基本QOSテーブル150Aと同一であるが、その属性値に関しては、基本QOSテーブル150Aで設定された値との差分を設定することができ。例えば、項番 (50) が"1"の場合を参照すると、属性抽出部14より入力されたServer (22) が"Server1"というプログラム名であった場合、損失優先度 (31) は基本QOSテーブル150Aにより規定される値"+1"に設定され、帯域 (33) は基本QOSテーブル150Aにより規定される値"+10%"に設定される。

[0102] 同様に、User-Agent (23) により規定されるクライアント名や、From (24) で規定されるユーザの電子メールアドレスによって、各コネクション品質 (31、32、33、34) を変更することにより、通信品質制御装置を使用するユーザとの契約条件に基づき最適なパラメータを設定することが可能である。項番 (50) が"4"の場合、"User2"という電子メールアドレスを持つユーザが"client2"というプログラム名を使用して動画通信を行なった場合には、遅延優先度 (31)、損失優先度 (32)、コネクション優先度 (34) が高く設定され、帯域 (33) も通常の3.0%多く設定されるため、より質の高い動画通信を実現可能である。

[0103] 項番 (50) が"5"の場合、送信元IP (42) がIPアドレス2であるユーザが"Server2"というサーバプログラムと通信を行なう場合に、図8に記されたコネクション品質が設定される。このよ

【0133】通信品質決定部15では、該Expireタイムアウトのチェックを行ない、現在時刻を経過している場合、セル損失低優先度を最低の0に設定する。もしくは、即座にデータグラムを廃棄する。

【0134】以上の制御により、データ作成後、時間の経過した価値の低いデータを優先的に廃棄する制御が可能である。

【0135】

【実施例7】レイヤ3がIPv4、レイヤ4がTCP、レイヤ5がSMTPであるデータグラムが入力された場合の実施例に関して説明する。

【0136】属性抽出部14は、レイヤ識別部13の出力よりレイヤ5がSMTPであることを認識し、SMTPのメールアドレスの“From:”フィールドが存在するかをチェックを行い、存在する場合その属性値と共に通信品質決定部15へ出力する。該“From:”フィールドより、メールの送信ユーザの電子メールアドレスを判別できる。

【0137】QOSデータグラム150には、契約したユーザに関連して、“From:”フィールドに対応する、遅延優先度(31)、損失率(32)、帯域(33)、コネクション優先度(34)、付加品質(35)、転送先VPI(42)等の値が設定されている。

【0138】通信品質決定部15では、QOSデータグラム150の検索を行ない、該“From:”フィールドのユーザ電子メールアドレスに対応するデータが存在するかどのチェックを行ない、存在する場合には設定されたコネクション品質、存在しない場合にはデフォルトのコネクション品質を決定する。

【0139】

【実施例8】レイヤ3がIPv4、レイヤ4がTCP、レイヤ5がFTPであるデータグラムが入力された場合の実施例に関して説明する。

【0140】図6にFTPクライアントによるファイル取得の例を示す。

【0141】図6の例では、ftpserverというホスト名のFTPサーバに対して、user1というユーザ名のユーザがログインし、“test.dat”というファイルを取得している。先頭の数字と“.”は、行数をあらわすために便宜的につけたものである。

【0142】“>”で始まる行は、クライアントがサーバに対してFTPコマンドを転送したことを意味しており、3桁の数字と一文字の空白で始まる行は、クライアントがサーバからFTPファイルを受信したことを意味している。

【0143】“test.dat”というファイルを取得する場合、ユーザが“get test.dat”というコマンドを入力(10行目)すると、クライアントは、サーバに対してまずPORTコマンドを出力(11行目)し、サーバはPORTコマンド成功のFTPリ

プライを受信(12行目)すると、サーバに対してPETRコマンドを出力(13行目)する。FTPクライアントでは通常利用のコネクションとデータ用のコネクションは別々に設定される。PORTコマンドはデータ転送に使用するTCPコネクションのクライアント側のIPアドレスとポート番号をサーバに伝えるためのコマンドであり、PETRコマンドは、クライアントがサーバに対してファイルを転送するように要求するためのコマンドである。

【0144】図6の例では、クライアント側のIPアドレスは140.252.13.34であり、ポート番号は1174(4×256+150)である。サーバは、PETRコマンドを受信するとPORTコマンドにより指定されたクライアントホストのポートに対してコネクションを接続し、該コネクションを確立すると、クライアントに対してFTPプライコード“150”のFTPプライを送信後、該コネクションを利用して指定されたファイルの転送を行なう。

【0145】属性抽出部14は、レイヤ識別部13の出力よりレイヤ5がFTPであることを認識し、データグラムがFTPコマンドであるか、FTPプライであるかの判別を行ない、コマンドまたはプライの識別を通信品質決定部15へ出力する。

【0146】通信品質決定部15は、送信元IP(42)によりFTP用の帯域増設サービスに該当しているユーザであるかどうかを判別する。登録ユーザであり、FTPコマンドまたはPORTコマンドであることを受信すると、PORTコマンドのフォーマットである、IPアドレスとポート番号を記録しておく。同一コネクションにおいて、次に、PETRコマンドを受信した場合、記録しておいたIPアドレスとポート番号と現在のコネクションにおける宛先のIPアドレスとポート番号により、サーバからクライアントへのファイル転送に使用されるコネクションをあらかじめ識別することができ。

【0147】以上によって、該サーバからクライアントへのファイル転送に使用されるコネクションの帯域(33)を大きく設定することにより、FTPのファイル転送におけるコネクションに対してのみ効率的に大きな帯域を割り当てることが可能である。

【0148】この際、通信品質決定部15は、ファイル転送に使用されるコネクションを識別するための情報と、該ファイル転送に使用されるコネクションに設定したコネクション品質をコネクション通信品質管理部17へ出力する。

【0149】コネクション通信品質管理部17は、該ファイル転送に使用されるコネクションに関連して、入力された該コネクション品質を基に通信品質を決定する。

【0150】

【0119】本実施例では、QOSデータベース150として基本QOSデータグラム150Aと拡張QOSデータグラム150Bを用いて、HTTPヘッダとIPヘッダから情報の属性値を検査し、コネクション品質を決定しているが、基本QOSデータグラム150Aのみを使用する運用も考えられる。その場合は、HTTPヘッダ内のContent-Typeのみでコネクション品質が決定される。

【0120】

【実施例9】本発明における通信データグラム転送装置において、課金を行なう場合の例に関して説明する。課金は、コネクション通信品質管理部17においてVCCコネクション単位で管理する。課金額は、“トラフィック量×基本課金額”より決定するものとする。また、トラフィック量は、VCCコネクション単位での通過するパケット数、もしくは転送バイト数、もしくは転送バイト数、もしくは総ビット数によってカウントされる。基本課金額はVCCコネクションのコネクション品質に応じて決定するものとする。

【0121】例えば、設定優先度(31)×重み1+損失率(32)×重み2+帯域(33)×重み3+コネクション優先度(35)×重み4+付加サービス量と設定する。付加サービス量は、例えばコネクションに対してL2TPなどのトンネリングアルゴリズムを適用した場合の追加料金である。

【0122】また、課金の対象となるユーザの限定方法に関して、レイヤ3以下の情報を用いる場合は、送信元IPアドレス、宛先IPアドレス等に限定されるが、レイヤ4以上の情報を用いることにより、例えば、HTTPヘッダのFrom、Server、User-Agent、Content-Typeを検査することにより、ユーザ電子メールアドレス、使用するサーバプログラム名、クライアントプログラム名、アプリケーション名等によりユーザ及び団体を特定することができ。

【0123】

【実施例3】属性抽出部14において、実施例1にてチェックするHTTPヘッダ以外に、新たにDateフィールドの存在チェックを行ない、存在する場合その属性値と共に通信品質決定部15へ出力する。該Dateフィールドより、データグラムの送信時間が取得される。

【0124】通信品質決定部15では、該Dateフィールドのチェックを行ない、設定されている属性値よりも時間が経過している場合、セル損失低優先度を最低の0に設定する。もしくは、即座にデータグラムを廃棄する。

【0125】以上の制御により、データ作成後、時間の経過した価値の低いデータを優先的に廃棄する制御が可能である。

【0126】また、通信品質決定部15で、前記Content-Typeが“audio”または“video”である場合に、該Dateフィールドのチェックを

行ない、設定されている属性よりも時間が経過している場合、セル損失低優先度を最低の0に設定する。もしくは、即座にデータグラムを廃棄する制御を行なうことにより、リアルタイムアプリケーションに関して、データ作成後、時間の経過した価値の低いデータを優先的に廃棄する制御が可能である。

【0127】

【実施例4】属性抽出部14において、実施例1もしくは実施例3にてチェックするHTTPヘッダ以外に、Authorizationヘッダフィールド、もしくはProxy-Authorizationヘッダフィールドの存在チェックを行ない、存在する場合その属性値を通信品質決定部15へ出力する。該Authorizationヘッダフィールド、もしくは、Proxy-Authorizationヘッダフィールドより、データグラムが認証情報を含んでいるかが判別できる。

【0128】通信品質決定部15では、Authorization-Authorizationヘッダフィールド、もしくはProxy-Authorizationヘッダフィールドが存在することを検出した場合、損失低優先度(32)を高く設定し、付加品質(34)としてデータグラムを符号化して転送することににより、認証情報を含まないデータに関連してより信頼性の高い通信を実現することが可能である。

【0129】

【実施例5】実施例4に関して、HTTPヘッダのAuthorizationヘッダフィールドが存在するかどうかを検出するだけでなく、属性値を検査し、適用されている認証情報を暗号化方法を認識することにより、より詳細に設定するコネクション品質を決定することも可能である。

【0130】以下、具体的に説明する。

【0131】通信品質制御部15は、Authorizationヘッダフィールドが入力された場合、Authorizationヘッダフィールド内の認証方法が“Basic”であるかどうかをチェックする。認証方法が“Basic”である場合、他の認証方法と比べてセキュリティが弱いため、損失低優先度(32)を高く設定して、付加品質(34)としてデータグラムを符号化して転送することにより、セキュリティの弱い認証方法である“Basic”を認証情報として含んでいるデータグラムについて、より信頼性の高い通信を実現することが可能である。

【0132】

【実施例6】属性抽出部14において、実施例1もしくは実施例3もしくは実施例4にてチェックするHTTPヘッダ以外に、新たにExpiresフィールドの存在チェックを行ない、存在する場合その属性値と共に通信品質決定部15へ出力する。該Expiresフィールドより、データグラムの有効日時を判別できる。

【0163】 属性抽出部15では、拡張QOSテーブルにURIの項目を追加する。

【0164】 属性抽出部15は、属性抽出部よりURIが入力されると、拡張QOSテーブルの検索を行い、テーブル内に入力されたURIが存在する場合、拡張QOSテーブルを参照することにより通信品質(Q)を決定する。URIが一致するかどうかのチェックが、フレイム単位で完全に一致するように良いが、登録する際のURIをDirectory単位に、属性抽出部より入力されるURIが登録URIの文字列を含む場合に一致すると判断しても良い。

【0165】 URIに対して通信品質を決定可能とすることにより、登録ユーザに対して、高度かつ多数な通信サービスを実現可能である。

【0166】 属性抽出部14においてHTTPヘッダから抽出するURIは、Request-Line内のRequest-URI以外に、Refererにより抜き出されるHTTPデータの参照元URI、Locationにより抜き出されるHTTPデータのおかれていURI、Forwardedにより抜き出されるデータグラムの転送先URI、Content-Baseにより抜き出されるデータグラムの転送元URI、Content-Locationにより抜き出されるURI、Cookieにより抜き出されるURIのいずれか、もしくは、全てであってもよい。

【0167】

【実施例13】 属性抽出部14において、受信データグラムがHTTPリクエストメッセージである場合にMethodの検査を行い、通信品質決定部15へ出力する。

【0168】 通信品質決定部15では、本通信データグラム転送装置から送信元IPアドレス方向に対するコネクションのための通信リソースをあらかじめ割り当てることにより、実際にServer側からHTTPリクエストメッセージを受信した場合、既に設定されているコネクション品質によりデータグラムをユーザ側へ転送することが可能である。

【0169】 設定するコネクション品質(S)として、MethodがGETもしくはPOSTである場合、帯域(33)を大きく設定する。MethodがGETもしくはPOSTである場合、MethodがHEADである場合に比べ情報量が大きいと考えられるため、帯域を有効に割り当てることが可能である。

【0170】

【実施例14】 属性抽出部14において、実施例1にてチェックするHTTPヘッダ以外に、新たにMIME-Versionのチェックを行ない、存在する場合その属性値と共に通信品質決定部15へ出力する。通信品質決定部15では、基本QOSテーブルにContent-type(21)に加え、該MIME-Version

nの項目を追加し、MIME-VersionとContent-typeの組によりコネクション品質を決定する。

【0171】

【実施例15】 属性抽出部14において、受信データグラムがHTTPリクエストメッセージである場合に、Accept、Accept-Charset、Accept-Encoding、Accept-Languageの検査を行い、存在する場合その属性値と共に通信品質決定部15へ出力する。

【0172】 通信品質決定部15では、あらかじめ契約を交わしているユーザの通信するWWWサーバに関してWebサーバのIPアドレス、Web Serverに対しての属性(51)、文字セット(52)、符号化方法(53)、言語(54)の情報をサーバ情報管理テーブル(500)に登録しておく、サーバ情報管理テーブル(500)の例を図10に示す。

【0173】 通信品質決定部15は、属性抽出部14より、Accept、Accept-Charset、Accept-Encoding、Accept-Languageのいずれかもしくは複数が入力されると転送するデータグラム内の宛先IPアドレス(41)がServer情報管理テーブル(500)に存在するかをチェックを行なう。宛先IPアドレス(41)が存在する場合、以下の処理を行なう。

【0174】 (1) Acceptの属性値がメディア属性(51)に登録されている属性値と一致するかどうかのチェックを行なう。宛先IPアドレス(41)がIPアドレス3である場合、テキストのメディア属性として、"text/plain"と"text/html"に対応している。Acceptの属性値が"text/plain"、"text/html"以外のテキストのメディア属性である場合、メディア属性(51)が一致していないと判断する。

【0175】 宛先IPアドレス(41)がIPアドレス3である場合は、他の画像や音声のメディア属性に関しては特に規定していない。宛先IPアドレス(41)がIPアドレス1、IPアドレス2の場合、サーバ情報管理テーブル(400)のメディア属性(51)は、"-"となっている。この場合、Web Serverの対応しているメディア属性(51)は登録されておらず、Acceptの属性値との比較は行なわない。

【0176】 (2) Accept-Charsetのメディア属性値が文字セット(52)と一致するかどうかのチェックを行なう。宛先IPアドレス(41)がIPアドレス1である場合、文字セット(52)として、"ISO-8859-1"のみに対応している。Accept-Charsetの属性値が"ISO-8859-1"以外である場合、文字セット(52)が一致していないと判断する。

伝えるFTPリトライを抽出し、さらに、FTPリトライ内部のリトライコードが"150"であることを抽出した際(14行)に、リトライコードに続くデータに記されているデータサイズを識別することにより、リトライサイズによって設定する帯域を変更するという運用も可能である。

【0151】

【実施例10】 属性抽出部14において、実施例1にてチェックするHTTPヘッダ以外に、新たにPragmaフィールド、もしくは、Cache-Controlフィールドのチェックを行ない、Pragmaフィールド、もしくは、Cache-Controlが存在し、その属性値が"no-cache"である場合、通信品質決定部15へ出力する。

【0152】 通信品質決定部15では、特定の宛先IPアドレス(41-1)で規定されるHTTP Serverへのアクセスに関して、キャッシュが使用可能である場合とキャッシュが使用できない場合に別々の経路を設定しておく。

【0153】 通信品質決定部15は、データグラム内の宛先IPアドレスが登録されている宛先IPアドレス(41-1)である場合、"no-cache"であるという情報が入力されているかどうかにより、キャッシュが使用可能であるかの判断を行ない、転送する経路を選択する。

【0154】 キャッシュを使用するかしないかにより経路を切り替えることにより、ネットワークを流れるトラフィックを分散し、キャッシュを使用しないコネクションに関しては高速度なデータアクセスを通過させるようにする等の制御が可能となる。

【0155】

【実施例11】 属性抽出部14において、受信データグラムがHTTPリクエストメッセージである場合、Request-Line内のRequest-URI、If-Modified-Sinceフィールド、If-Unmodified-Sinceフィールドのチェックを行い、存在する場合その属性値と共に通信品質決定部15へ出力する。

【0156】 本通信データグラム転送装置の提供するサービスとあらかじめ契約しているユーザは、管理しているWWWサーバにおいて、頻繁にIf-Modified-Since、もしくは、If-Unmodified-SinceフィールドによるチェックのありそうなURIとその更新時間を登録しておく。通信品質決定部15において、登録されたURIとその更新時間のテーブルを管理する。

【0157】 通信品質決定部15は、Request-URIが登録されているURIと一致し、If-Modified-Sinceフィールド、もしくは、If-Unmodified-Sinceフィールドの属性値

が入力されている場合に、その属性値とテーブルより参照される最終更新時間を比較する。

【0158】 If-Modified-Sinceフィールドより取得される日時が該URIの最終更新時間より古い場合、もしくは、If-Unmodified-Sinceフィールドより取得される日時が、最終決定部により出力されるデータグラム転送先経路(R)へデータグラム(D)を転送する。

【0159】 If-Modified-Sinceフィールドにより取得される日時が該URIの最終更新時間より古い場合、データグラムの損失優先度(32)を低く設定する。もしくは、該データグラムの優先度、Status Codeが304(not modified)であるHTTPレスポンスメッセージを作成し、送信元IPアドレスに対して転送する。

【0160】 If-Unmodified-Sinceフィールドより取得される日時が該URIの最終更新日時より新しい場合、データグラムの損失優先度(32)を低く設定する。もしくは、データグラム優先度、Status Codeが412(Precondition Failed)であるHTTPレスポンスメッセージを作成し、送信元IPアドレスに対して転送する。

【0161】 以上により、不要なトラフィックをサーバ及びネットワーク内に転送しないようにする事が可能である。

【0162】 また、あらかじめURIを登録しておく方法以外にも受信したデータグラム(D)がHTTPレスポンスメッセージであり、該データグラムのHTTPヘッダ内にLast-Modifiedヘッダが存在する場合、URI(U)とLast-Modifiedヘッダより得られる最終更新時間の値を登録する方法も考えられる。該URIは、ユーザ端末からWWWサーバへのHTTPリクエストメッセージ内のRequest-URI、もしくは、Request-URIとHostヘッダより抽出される、HTTPリクエストメッセージとHTTPレスポンスメッセージの対応付けは、HTTPリクエストメッセージもしくはHTTPレスポンスメッセージを構成するデータグラム(D)のコネクション情報(C)より判断される。(リクエストメッセージとしては、実施例20を参照のこと)登録するURIは、あらかじめ契約しているユーザのサーバもしくはサーバ内の特定ディレクトリに限定しても良い。すべてのURIを対象としても良い。

【実施例12】 属性抽出部14において、受信データグラムがHTTPリクエストメッセージである場合に、実施例1にてチェックするHTTPヘッダ以外に、Request-LineのRequest-URIのチェックを行ない、属性値として読み出されるURIを通信品質決定部15へ出力する。

が端末とProxyサーバ間のデータグラムに関してより信頼性の高い通信を実現することが可能である。

[0192]

[実施例20] 本発明の実施例20の形態について図面を参照して詳細に説明する。

[0193] 図11は、本発明の実施例20における通信データグラム転送装置1Aの構成例を示すブロック図である。

[0194] 属性抽出部14は、受信データグラム(D)がHTTPリクエストメッセージである場合、HTTPヘッダ内のリクエストURI、もしくは、リクエストURIとHostヘッダフィールドより、アクセスするWWWサーバへのabsolute-URI(70)を抽出し、通信品質決定部15Aへ出力する。

[0195] 通信品質決定部15Aは、コネクション識別部13より入力されるコネクション情報(C)と属性抽出部14より入力される該URI(70)とを相対してコネクション情報管理テーブル151に登録する。

[0196] 属性抽出部14において、受信データグラムがHTTPリクエストメッセージである場合、HTTPヘッダ内にAllowフィールド、Accept-Rangeフィールド、Content-Locationフィールドが存在するかの検査を行い、存在する場合その属性値と共に通信品質決定部15Aへ出力する。

[0197] 通信品質決定部15Aは、HTTPヘッダ内のAllowフィールド、Accept-Rangeフィールドのどちらかもしくは両方が入力された場合、Content-Baseフィールドが入力されたかどうかをチェックし、Content-Baseフィールドが入力されている場合、URIフィールド152に、Content-Baseフィールド内の属性値であるabsolute-URIとAllowフィールド内の許可マスコッド(80)、Accept-Rangeフィールド内の許可レンジ(81)を相対して登録する。

[0198] Content-Baseフィールドが入力されていない場合、Content-Locationフィールドが入力されているかどうかをチェックし、Content-Locationフィールドが入力されている場合、URIフィールド152に、Content-Locationフィールド内の属性値であるabsolute-URIとAllowフィールド内の許可マスコッド(80)、Accept-Rangeフィールド内の許可レンジ(81)を相対して登録する。

[0199] Content-Locationフィールドが入力されていない場合、コネクション情報管理テーブル151より、コネクション情報(C)に対応するURI(70)を読み出し、URIフィールド152にURI(70)とAllowフィールド内の許可マスコッド(80)、Accept-Rangeフィールド内の許

可レンジ(81)を相対して登録する。

[0200] 属性抽出部14は、受信データグラムがHTTPリクエストメッセージである場合、HTTPヘッダ内のマスコッド(71)を抽出し、通信品質決定部15Aへ出力する。

[0201] 属性抽出部14は、受信データグラムがHTTPリクエストメッセージである場合、HTTPヘッダ内のRangeヘッダ、もしくは、If-Rangeヘッダが存在するかのチェックを行い、存在する場合、Rangeヘッダ、もしくは、If-Rangeヘッダの属性値であるレンジ(72)を抽出し、通信品質決定部15Aへ出力する。

[0202] 通信品質決定部15Aは、属性抽出部14より前記URI(70)が入力されるとURIフィールド152の検査を行い、該URIに対する許可マスコッド(80)もしくは許可レンジ(81)が登録されていないかを検索する。

[0203] 許可マスコッド(80)が登録されている場合、属性抽出部14より入力されるマスコッド(71)との比較を行なう。比較の結果、マスコッド(71)が登録されていない場合、データグラム(D)を廃棄する。もしくは、廃棄後、Status Codeが405(Method Not Allowed)であるHTTPリクエストメッセージを作成し、送信元IPアドレスに対して転送する。

[0204] 許可レンジ(81)が登録されており、属性抽出部14よりレンジ(72)が入力された場合、許可レンジ(81)とレンジ(72)の比較を行なう。比較の結果、レンジ(72)による要求方法が許可レンジ(81)に登録されているもので無い場合、付加品質(35)としてデータグラム(D)内に存在するRangeヘッダに関連するヘッダを除去するように設定する。

[0205] 出力キュー管理部12においてRangeヘッダに関連するヘッダが除去される。

[0206] 除去されるヘッダは、データグラム(D)がRangeヘッダを含む場合は、Rangeヘッダ、If-Unmodified-Sinceヘッダ、If-Matchヘッダであり、データグラム(D)がIf-Rangeヘッダを含む場合は、If-Rangeヘッダのみである。

[0207]

[実施例21] この実施例21の基本的構成については、実施例20と同一である。ただし、URIフィールド152の代わりにWWWサーバフィールド153を使用する。

[0208] 属性抽出部14において、受信データグラムがHTTPリクエストメッセージである場合に、HTTPヘッダ内のPublicフィールドの検査を行い、存在する場合その属性値と共に通信品質決定部15

[0177] (3) Accept-Encodingの属性値が符号化方法(53)と一致するかどうかのチェックを行なう。宛先IPアドレス(41)がIPアドレスもしくはIPアドレス2である場合、符号化方法(53)として、"gzip"、"compress"に対応している。Accept-Encodingの属性値が"gzip"、"compress"以外である場合、符号化方法(53)が一致していないと判断する。

[0178] 宛先IPアドレス(41)がIPアドレス3である場合、符号化方法(53)は"x"となっている。この場合、Web Serverはどの符号化方法(53)にも対応していないことになり、この場合、Accept-Encoding属性値が何であっても、符号化方法(53)は一致していないと判断する。

[0179] (4) Accept-Languageの属性値が言語(54)と一致するかどうかのチェックを行なう。言語(54)がIPアドレス1である場合、言語(54)として、"en"、"jp"に対応している。Accept-Languageの属性値が"en"、"jp"以外である場合、言語(54)は一致していないと判断される。

[0180] 通信品質決定部15が、上記処理において、メディア属性(51)、文字セット(52)、符号化方法(53)、言語(54)のいずれかもしくは複数において、一致しないと判定した場合、該データグラムを廃棄し、Status Codeが406(Not Acceptable)であるHTTPリクエストメッセージを作成し、送信元IPアドレスに対して転送する。

[0181] 実施例15は、WWWサーバ側の対応可能なメディア属性(51)、文字セット(52)、符号化方法(53)、言語(54)を登録しておき、一致しないメッセージを廃棄する制御であるが、クライアント側の対応可能なメディア属性(51)、文字セット(52)、符号化方法(53)、言語(54)を登録する方法も考えられる。

[0182] その場合、HTTPリクエストメッセージにおいて、Content-Type内のメディア属性(51)、Content-Encoding内の符号化方法(53)、Content-Language内の言語(54)から抽出した属性値が登録されていない場合、該コネクションに関するデータグラムを廃棄する。もしくは、損失率を低く設定することにより、無駄なトラフィックをネットワークに転送しないようにすることが可能である。

[0183]

[実施例16] 属性抽出部14において、受信データグラムがHTTPリクエストメッセージである場合、Status Codeのチェックを行い、その属性値と共に通信品質決定部15へ出力する。

[0184] 通信品質決定部15は、Status Codeが入力されるとその属性値が200(OK)である場合のみ、帯域(33)を大きく設定する。

[0185] Status Codeが200(OK)である場合のみ、該データグラムで規定されるコネクションにおいて多くのデータグラムが転送されることが予想されるため、効率的に帯域を割り当てることが可能となる。

[0186]

[実施例17] 属性抽出部14において、受信データグラムがHTTPリクエストメッセージである場合、HTTPヘッダ内にWWW-Authenticateヘッダが含まれるかどうかのチェックを行ない、通信品質決定部15へ出力する。

[0187] WWW-Authenticateヘッダを含むデータグラムが転送された場合、その後、認証情報を含むデータグラム、もしくは、認証後にWWWサーバから受信したデータグラムが含まれている可能性がある。

[0188] 通信品質決定部15は受信データグラム(D-17)がWWW-Authenticateヘッダを含んでいるという情報が入力されると、該データグラム(D-17)に含まれる宛先IPアドレス(41)、送信元IPアドレス(42)より、ユーザ端末とWWWサーバ間のHTTPコネクションに対して、一定期間、損失優先度(32)を高く設定し、付加品質(34)としてデータグラムを符号化して転送するようにコネクション品質(S)を決定することにより、ユーザ端末とWWWサーバ間のデータグラムに関してより信頼性の高い通信を実現することが可能である。

[0189]

[実施例18] 属性抽出部14において、受信データグラムがHTTPリクエストメッセージである場合、HTTPヘッダ内にProxy-Authenticateヘッダが含まれるかどうかのチェックを行ない、通信品質決定部15へ出力する。

[0190] Proxy-Authenticateヘッダを含むデータグラムが転送された場合、その後、認証情報を含むデータグラム、もしくは、認証後にProxyサーバから受信したデータグラムが含まれている可能性がある。

[0191] 通信品質決定部15は受信データグラム(D-18)がProxy-Authenticateヘッダを含んでいるという情報が入力されると、該データグラム(D-18)に含まれる宛先IPアドレス(41)、送信元IPアドレス(42)より、ユーザ端末とProxyサーバ間のHTTPコネクションに対して、一定期間、損失優先度(32)を高く設定し、付加品質(34)としてデータグラムを符号化して転送するようにコネクション品質(S)を決定することにより、ユー

[02301]

【実施例29】受信データグラムのレイヤ4がUDPである場合、属性検出部14は、UDPヘッダのchecksumフィールドを検査し値が0であるかどうかをチェツクし、通信品質決定部15へ出力する。

【0231】通信品質決定部15は、checksumフィールドの値が0であることを入力することににより、該データグラムがチェツクサムを利用していないことを認識する。該データグラムの宛先IPアドレス、もしくは、転送元IPアドレスがあらかじめ登録されているユーザのIPアドレスと一致する場合、損失優先度を高く設定し、可能であれば、付加品質としてデータエラーの発生しにくい専用の物理回線を利用するように設定する。

【0232】以上の制御によりチェツクサムを使用しないUDP通信においても、契約しているユーザに対しては信頼性の高い通信を提供することが可能である。

[0233]

【実施例30】受信データグラムのレイヤ5がDNSである場合、属性検出部14は、query typeが存在するかをチェツクを行ない、query typeが存在する場合通信品質決定部15へ出力する。

【0234】通信品質決定部15は、query typeが入力されると、値が252であるかをチェツクする。

【0235】値が252である場合、zone transfer要求であり、他のDNSメッセージに比べ多くのデータグラムが転送されることが予想されるため、帯域(33)を大きく設定する。

[0236]

【実施例31】受信データグラムのレイヤ5がFTPである場合、属性検出部14は、FTPメッセージに含まれるopcodeを検査し、通信品質決定部15へ出力する。

【0237】属性検出部14は、UDPヘッダに含まれるUDPポートの検出を行ない、通信品質決定部15へ出力する。

【0238】通信品質決定部15は、opcodeが入力されると値が3であるかをチェツクを行なう。

【0239】opcodeが3であり、かつ、UDPポートより算出されるFTPメッセージの長さが512である場合、FTPによりデータの転送が行なわれていることが判別できるので、帯域(33)を大きく設定する。

【0240】opcodeが3であり、かつ、UDPポートより算出されるFTPメッセージの長さが512より小さい場合、FTPによりデータの転送が完了したことが判別できるので、帯域(33)を小さく設定する。

【0241】以上の制御により、データ転送時のみ帯域

を大きく割り当てることができるとある。

[0242]

【実施例32】受信データグラムのレイヤ5がSNMPである場合、属性検出部14は、SNMPメッセージに含まれるPDUタイプを検査し、通信品質決定部15へ出力する。

【0243】通信品質決定部15は、PDUタイプのチェツクを行ない、PDUタイプが4である場合、SNMPメッセージがトラップメッセージであることを認識し、該データグラムの遅延優先度(31)を高く設定することにより、トラップメッセージを高速に転送することが可能である。

[0244]

【実施例33】本実施例では、実施例1に加え、通信品質決定部15において決定するコネクシオン通信品質(S)に、新たにコネクシオン設定ロバストネス(強度)(37)を追加する。予め契約しているユーザは、3段階のコネクシオン設定ロバストネス(37)の中から1つを選択して設定することができ、

【0245】コネクシオン通信品質管理部17では、入力されたコネクシオン設定ロバストネス(37)に基づき、通信品質制御装置6a、6b、6c、6d間のコネクシオン(図12)を以下のように設定する。

【0246】(1) コネクシオン設定ロバストネス=1の場合(図13)、通信品質制御装置6aは、コネクシオンを設定するために必要な情報を持つコネクシオン設定メッセージを送信すると同時に、データグラムの転送を開始する。通信品質制御装置6b、6cは、コネクシオン設定メッセージを受信すると、通信品質制御装置6c、6dに対してコネクシオン設定メッセージを送信すると同時に、受信したデータグラムを転送する。

【0247】(2) コネクシオン設定ロバストネス=2の場合(図14)、通信品質制御装置6aは、コネクシオンを設定するために必要な情報を持つコネクシオン設定メッセージを送信する。通信品質制御装置6b、6c、6dは、コネクシオン設定メッセージを受信した場合、予め定められた条件でコネクシオン設定が可能であれば、送信元の通信品質制御装置6a、6b、6cに対して、ACKメッセージを送信する。通信品質制御装置6b、6cは、ACKメッセージを受信後、コネクシオン設定メッセージを通信品質制御装置6c、6dに送信する。通信品質制御装置6a、6b、6cは、ACKメッセージを受信後、データグラム転送を開始する。以上により、データグラムは転送を開始する通信品質制御装置とのコネクシオンが確立してから転送される。

【0248】(3) コネクシオン設定ロバストネス=3の場合(図15)、通信品質制御装置6aは、コネクシオンを設定するために必要な情報を持つコネクシオン設定メッセージを送信する。通信品質制御装置6b、6cは、コネクシオン設定メッセージを受信した場合、予め

Aに出力する。

【0209】通信品質決定部15Aは、HTTPヘッダ内のPublicフィールドが入力されると、Content-Baseフィールドの属性値であるURI、もしくは、Content-Locationフィールドの属性値であるURI、もしくは、コネクシオン情報管理フィールド151より読み出されたURI(70)のいずれかよりWWWサーバのホスト名(700)を抽出し、WWWサーバ-グループ153にホスト名(700)とPublicフィールド内の許可マスト(800)を紐付けて登録する。

【0210】通信品質決定部15Aは、属性検出部14よりURI(70)が入力されるとWWWサーバ-グループ153の検索を行ない、該URI(70)より抽出されるWWWサーバホスト名(700)に対応する許可マスト(800)が登録されているかを検索する。

【0211】許可マスト(800)が登録されている場合、属性検出部14より入力されるマスト(71)との比較を行なう。比較の結果、マスト(71)が登録されていない場合、データグラム(D)を廃棄する。もしくは、廃棄後、Status Codeが405(Method Not Allowed)であるHTTPメソッドメッセージを作成し、送信元IPアドレスに対して転送する。

[0212]

【実施例22】レイヤ5がHTTPである場合の上記各実施例に以下の制御を追加することが可能である。

【0213】HTTPボンスメッセージにContent-Lengthが含まれていることを検出した場合、Content-Lengthの長さに応じて、帯域(33)を割り当てる。

[0214]

【実施例23】レイヤ5がHTTPである場合の上記各実施例に以下の制御を追加することが可能である。

【0215】HTTPボンスメッセージにConnectionが含まれていることを検出した場合、Connectionの属性値がpersistentである場合に、帯域(33)を大きく割り当てる。

【0216】Connectionの属性値がpersistentである場合、他の属性値である場合に比べ多くのデータグラムが転送されると予想されるため効率的なデータグラム転送が可能である。

[0217]

【実施例24】レイヤ5がHTTPである場合の上記各実施例に以下の制御を追加することが可能である。

【0218】HTTPボンスメッセージにWarningヘッダが含まれていることを検出した場合に、WarningヘッダのWarning-codeが10(Response is stale)である場合、喪失優先度を低く設定することにより、日時の古いデータ

グラムを優先的に廃棄することが可能である。

[0219]

【実施例25】レイヤ5がHTTPである場合の上記各実施例に以下の制御を追加することが可能である。

【0220】HTTPボンスメッセージにRetry-Afterヘッダが含まれていることを検出した場合、Retry-Afterより次に要求したURIにアクセス可能時間を抽出し、URI(70)と該アクセス可能時間を紐付けてURI-グループに登録する。

【0221】次に、同一のURI(70)に対してアクセスがあった場合、該URI-グループより前記アクセス可能時間を読み出し、データグラムを受信した時刻よりも先である場合、データグラムを廃棄する。

【0222】データグラムを受信してから実際にWWWサーバにデータグラムが転送されるまでの時間を算出可能である場合は、WWWサーバにデータグラムが転送される時間との比較を行なっても良い。

[0223]

【実施例26】レイヤ5がHTTPである場合の上記各実施例に以下の制御を追加することが可能である。

【0224】HTTPヘッダ内にViaヘッダを抽出した場合、Viaヘッダ内にあらかじめ登録されているホスト名、プログラム名が含まれている場合、プログラムに登録してある通信品質(S)を設定し、データグラムを転送する。

【0225】以上の制御により通過するproxyにおけるホスト名、プログラム名によって契約内容に応じた通信品質を提供することが可能である。

[0226]

【実施例27】属性検出部は、受信データグラム(D)がHTTPボンスメッセージであり、あらかじめ登録されているユーザ宛のIPアドレスである場合、HTTPヘッダ内のTransfer-Encodingヘッダのチェツクを行なう。Transfer-Encodingヘッダが存在しない場合、受信データグラム(D)の属するコネクシオンに対して付加品質(35)としてデータグラムを符号化して転送するように設定する。

【0227】以上の制御により、Transfer-Encodingヘッダが存在しない、セキエリテの弱いデータグラムを安全に転送することが可能である。

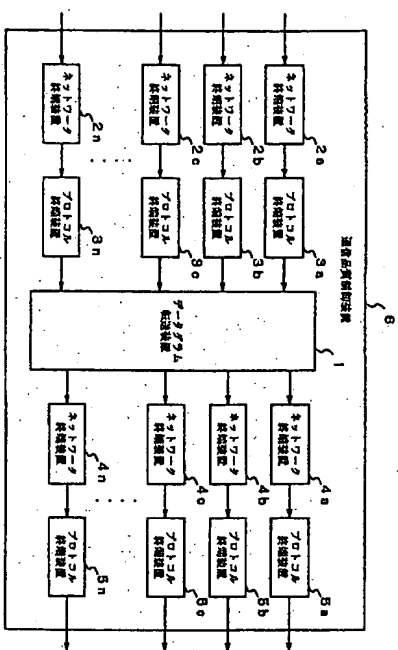
[0228]

【実施例28】受信データグラムのレイヤ4がTCPである場合、属性検出部14は、TCPヘッダのCode bitで決定するURG(URGent)をチェツクし、通信品質決定部15へ出力する。

【0229】通信品質決定部15は、URGフィールドに1が設定されている場合、緊急メッセージであると判断し、遅延優先度、喪失優先度を高く設定することにより、高速で信頼性の高い通信品質を提供する。

【図15】 通信品質制御装置間の接続設定例を説明するブロック図である。

- 【符号の説明】
- 1、1A 通信データグラム転送装置
 - 2a、2b、2c、...、2n ネットワーク転送装置
 - 5a、5b、5c、...、5n ネットワーク転送装置
 - 3a、3b、3c、...、3n プロトコル転送装置
 - 4a、4b、4c、...、4n プロトコル転送装置
 - 6 通信品質制御装置
 - 11 入力キュー管理部
 - 12 出力キュー管理部
 - 13 レイヤ識別部
 - 14 属性抽出部
 - 15、15A 通信品質決定部
 - 16 経路決定部
 - 150 QoSデータベース
 - 151 コネクション管理テーブル
 - 152 URIテーブル
 - 160 経路テーブル
 - 21 Content-type
 - 22 Server
 - 23 User-Agent



【図15】

- 24 From
- 31 遅延優先度
- 32 損失優先度
- 33 帯域
- 34 コネクション優先度
- 35 付加品質
- 36 転送先VPI
- 41 宛先IP
- 42 送信元IP
- 43 宛先サブネットワークアドレス
- D 転送されるデータグラム
- C データグラムより抽出したコネクション情報
- A 経路決定部が経路を決定するために必要な情報
- L データグラムの一部もしくは全部
- DP 属性抽出部より検査された属性情報
- P 通信品質決定部において検査されたコネクション情報
- R データグラムの転送先経路
- Q、Q1、Q2、Q3、Q4 データグラムを転送するための通信品質

定められた条件でコネクション設定が可能であれば、送信先の通信品質制御装置6c、6dに対してコネクション設定メッセージを作成して送信する。通信品質制御装置6dは、コネクション設定メッセージを受信した場合、予め定められた条件でコネクション設定が可能である場合、送信元の通信品質制御装置6cに対してACKメッセージを送信する。通信品質制御装置6c、6bは、ACKメッセージを受信すると通信品質制御装置6b、6aに対してACKメッセージを送信する。通信品質制御装置6aは、ACKメッセージを受信後、データグラム転送を開始する。以上により、データグラムは通信品質制御装置6a、6b、6c、6d間までのコネクションが完全に確立してから転送されるため、信頼性の高いデータグラム転送が可能となる。

【0249】 以上のように、コネクション設定ロバストネスが大きいほどデータグラムが確実に転送されること保証される。ユーザは転送するデータグラムの要求品質に合わせてコネクション設定ロバストネスを選択する。

【0250】 なお、本発明は上述した実施の形態に限定されるのではなく、その技術思想の範囲内において様々な変形して実施することができる。

【0251】

【発明の効果】 以上説明したように本発明の通信品質制御装置によれば、以下に述べるような効果が得られる。

【0252】 第1に、通信のメディア属性に応じた通信の品質を決定することができる。その理由は、例えばHTTPヘッダにおけるContent-type等のデータグラムにおけるレイヤ5の部分の属性を抜き出すことにより、画像、音声、動画、アプリケーションといったコネクションの属性を識別でき、それぞれに適したコネクション品質に応じて通信ができるからである。

【0253】 第2に、あらかじめ登録してあるユーザに対して高度かつ多様な通信サービスを実現できる。その理由は、例えばHTTPヘッダにおけるServer、User-Agent、FromやSMTPにおけるメールアドレスのFrom行などにより、データグラムを送信した、もしくは、送信先のユーザ名や使用クライアントソフト名、サーバソフト名等を特定することができる。あらかじめ登録しているユーザやソフト製作者会社に対して、契約内容に基づくコネクション品質を適用してデータグラムの転送を行なうことができるからである。

【0254】 第3に、通信品質に応じた料金で転送を行なうことができる。その理由は、レイヤ4以上により取得される通信属性に対応するコネクション品質に応じて料金を行なう際のレートもしくは基本料金を決定することができるからである。

【0255】 第4に、データグラムがセキュリティ上非常に重要なデータを含んでいるかどうかを判断し、データグラムに対応するセキュリティ品質に応じたデータ転送を実現できる。その理由は、例えばHTTPヘッダにおいてAuthorizationヘッダフィールドが存在するかどうかを判断することにより、データグラムが認証情報を含んでいるかどうかを抽出することができるからである。

【0256】 第5に、データグラムの新規性を判断し、コネクションの品質を決定することができる。その理由は、例えばHTTPヘッダにおけるDateやExpires等のデータグラムの作成日時や有効期限などの情報により、時間の観点からデータグラムの重要性を判断でき、古くなったデータを優先的に廃棄する制御を実現可能であるからである。

【0257】 第6に、同一のコネクションで認識できる情報だけでなく、他のコネクションにおいて認識した情報を基にコネクション品質を決定し、最適な通信品質でデータグラムを転送可能である。その理由は、例えばFTPアプリケーションのデータグラムが送受信されている際に、FTPコマンドやFTPリプライの内容を識別することにより、新たにファイル転送を行なうための別のコネクションが設定されたことを識別することができ、ファイル転送時にのみ大きな帯域を割り当てるといった制御が可能だからである。

【図面の簡単な説明】

【図1】 本発明の実施の形態における通信品質制御装置の構成例を示すブロック図である。

【図2】 本発明の実施の形態における通信データグラム転送装置の構成例を示すブロック図である。

【図3】 本発明の実施の形態におけるレイヤ識別部の動作を説明するフローチャートである。

【図4】 本発明の実施の形態におけるコネクション通信品質管理部の動作を説明するフローチャートである。

【図5】 HTTPセッションをIPデータグラムに分割化する場合の例を示す図である。

【図6】 FTPによるファイル転送の例を示す図である。

【図7】 QoSデータベース内の基本QoSテーブル例を説明する図である。

【図8】 QoSデータベース内の拡張QoSテーブル例を説明する図である。

【図9】 経路テーブルの例を説明する図である。

【図10】 サーバ情報管理テーブルの例を説明する図である。

【図11】 通信データグラム転送装置の他の構成例を説明するブロック図である。

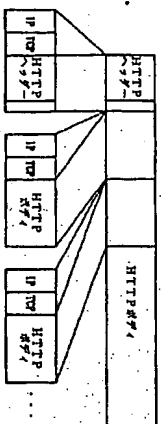
【図12】 通信品質制御装置間のコネクション設定例を説明するブロック図である。

【図13】 通信品質制御装置間のコネクション設定例を説明するブロック図である。

【図14】 通信品質制御装置間のコネクション設定例を説明するブロック図である。

【図5】

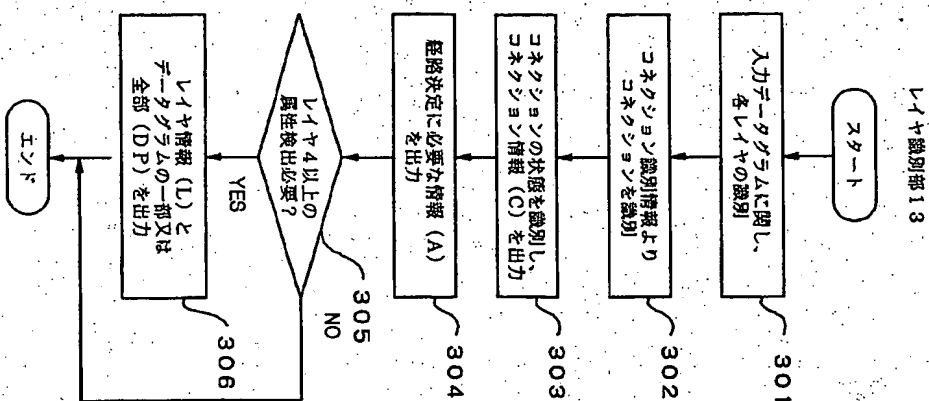
【図7】



基本QoSデータベース

Content-type (2.1)	遅延優先度 (3.1)	損失優先度 (3.2)	帯域 (3.3)	コネクション 優先度 (3.4)
image/*	1	2	4	1
audio/*	3	1	4	1
video/*	3	2	4	1
その他	2	3	4	2

[図3]

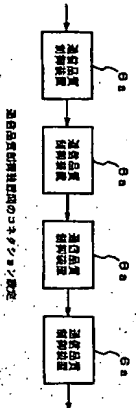


[図10]

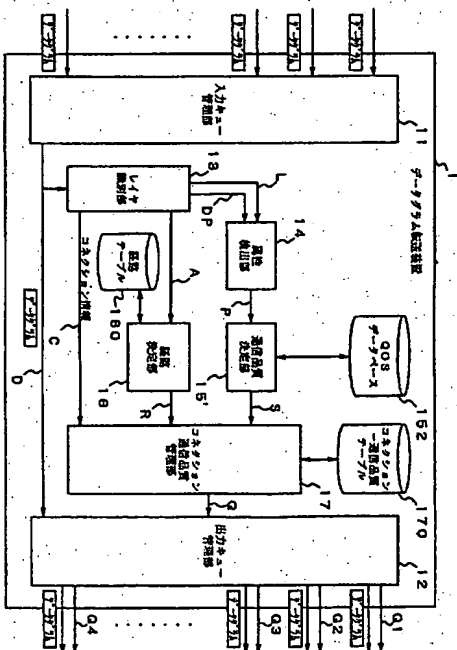
レイヤ4以上の属性検出テーブル

レイヤ	IP (5.1)	IP 属性 (5.2)	IP 属性 (5.3)	IP 属性 (5.4)
IPV4	-	-	10-450-1	0-15
IPV4	-	-	0-15	0-15
IPV4	-	-	0-15	0-15
IPV4	-	-	0-15	0-15

[図12]



[図2]



[図6]

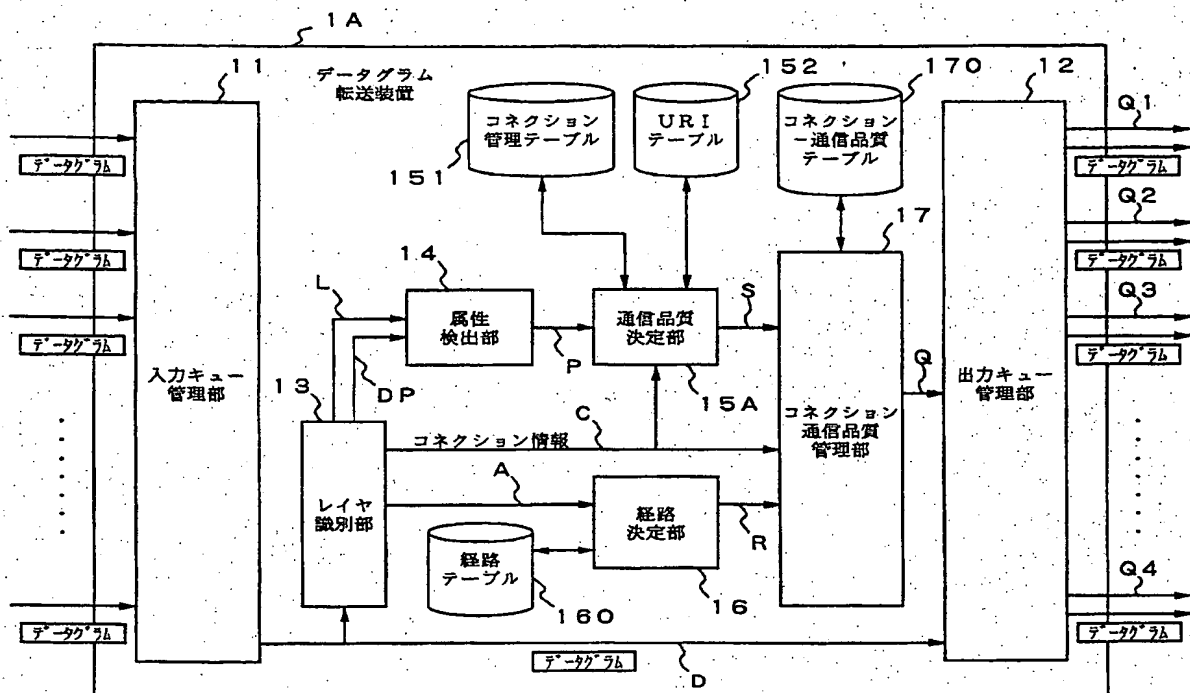
[図9]

1: Send to IP-4 layer
2: Send to IP-4 layer
3: Send to IP-4 layer
4: Send to IP-4 layer
5: Send to IP-4 layer
6: Send to IP-4 layer
7: Send to IP-4 layer
8: Send to IP-4 layer
9: Send to IP-4 layer
10: Send to IP-4 layer
11: Send to IP-4 layer
12: Send to IP-4 layer
13: Send to IP-4 layer
14: Send to IP-4 layer
15: Send to IP-4 layer
16: Send to IP-4 layer
17: Send to IP-4 layer
18: Send to IP-4 layer
19: Send to IP-4 layer
20: Send to IP-4 layer
21: Send to IP-4 layer
22: Send to IP-4 layer
23: Send to IP-4 layer
24: Send to IP-4 layer
25: Send to IP-4 layer
26: Send to IP-4 layer
27: Send to IP-4 layer
28: Send to IP-4 layer
29: Send to IP-4 layer
30: Send to IP-4 layer
31: Send to IP-4 layer
32: Send to IP-4 layer
33: Send to IP-4 layer
34: Send to IP-4 layer
35: Send to IP-4 layer
36: Send to IP-4 layer
37: Send to IP-4 layer
38: Send to IP-4 layer
39: Send to IP-4 layer
40: Send to IP-4 layer
41: Send to IP-4 layer
42: Send to IP-4 layer
43: Send to IP-4 layer
44: Send to IP-4 layer
45: Send to IP-4 layer
46: Send to IP-4 layer
47: Send to IP-4 layer
48: Send to IP-4 layer
49: Send to IP-4 layer
50: Send to IP-4 layer
51: Send to IP-4 layer
52: Send to IP-4 layer
53: Send to IP-4 layer
54: Send to IP-4 layer
55: Send to IP-4 layer
56: Send to IP-4 layer
57: Send to IP-4 layer
58: Send to IP-4 layer
59: Send to IP-4 layer
60: Send to IP-4 layer
61: Send to IP-4 layer
62: Send to IP-4 layer
63: Send to IP-4 layer
64: Send to IP-4 layer
65: Send to IP-4 layer
66: Send to IP-4 layer
67: Send to IP-4 layer
68: Send to IP-4 layer
69: Send to IP-4 layer
70: Send to IP-4 layer
71: Send to IP-4 layer
72: Send to IP-4 layer
73: Send to IP-4 layer
74: Send to IP-4 layer
75: Send to IP-4 layer
76: Send to IP-4 layer
77: Send to IP-4 layer
78: Send to IP-4 layer
79: Send to IP-4 layer
80: Send to IP-4 layer
81: Send to IP-4 layer
82: Send to IP-4 layer
83: Send to IP-4 layer
84: Send to IP-4 layer
85: Send to IP-4 layer
86: Send to IP-4 layer
87: Send to IP-4 layer
88: Send to IP-4 layer
89: Send to IP-4 layer
90: Send to IP-4 layer
91: Send to IP-4 layer
92: Send to IP-4 layer
93: Send to IP-4 layer
94: Send to IP-4 layer
95: Send to IP-4 layer
96: Send to IP-4 layer
97: Send to IP-4 layer
98: Send to IP-4 layer
99: Send to IP-4 layer
100: Send to IP-4 layer

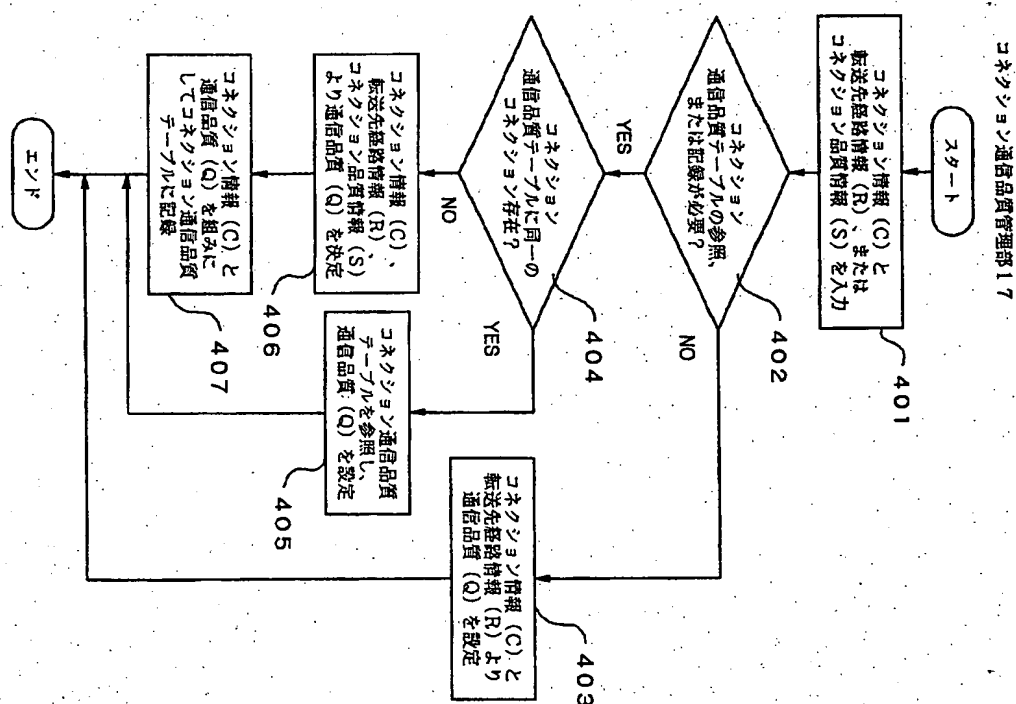
[図8]

レイヤ4以上の属性検出テーブル

レイヤ	IP (5.1)	IP 属性 (5.2)	IP 属性 (5.3)	IP 属性 (5.4)
IPV4	-	-	10-450-1	0-15
IPV4	-	-	0-15	0-15
IPV4	-	-	0-15	0-15
IPV4	-	-	0-15	0-15

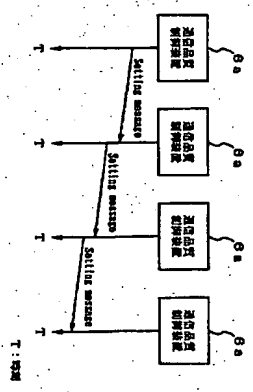


【図11】



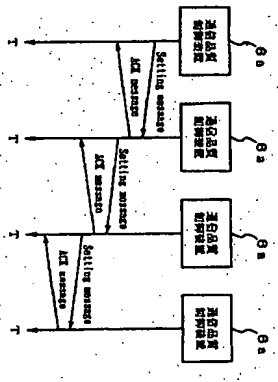
【図4】

【図13】



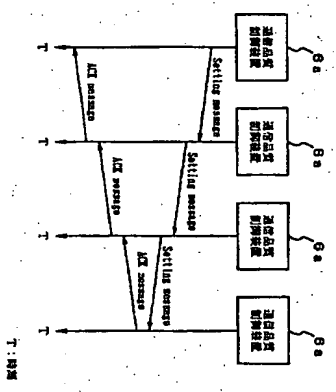
コネクション設定ロバトス=1の時のコネクション設定手順

【図14】



コネクション設定ロバトス=3の時のコネクション設定手順

【図15】



コネクション設定ロバトス=2の時のコネクション設定手順

フロントページの続き

(72) 発明者 阿留多伎 明良
東京都港区芝五丁目7番1号 日本電気株式会社内

Fターム(参考) SK030 GA11 GA16 GA19 HA10 HB08
HB16 HB18 HB21 HC14 HD03
HD06 JA07 JA08 KA05 KA07
KA17 KX29 LA03 LA05 LC05
LC13 LD20
SK033 AA04 AA08 AA09 BA15 CB01
CB08 CB17 DA03 DA05 DB16
DB19